이학석사 학위논문

압수한 디지털 데이터의 안전한 관리 방식 제안

2016년 12월

서울대학교 융합과학기술대학원

수리정보학과 디지털포렌식학

임 성 훈

압수한 디지털 데이터의
안전한 관리 방식 제안

지도교수 이 효 원

이 논문을 이학석사 학위논문으로 제출함

2016년 12월

서울대학교 융합과학기술대학원

수리정보과학과 디지털포렌식학

임 성 훈

임성훈의 석사 학위논문을 인준함

2016년 12월

위 원 장 엄 현 상 (인)

부위원장 이 효 원 (인)

위 원 천 정 희 (인)

요약(국문초록)

디지털 기기의 사용이 대중화 되면서, 우리가 인식하지 못하는 사이에 사람의 행동이 디지털 형태로 기록되는 경우가 점점 많아지고 있다. 많은 정보들이 디지털 데이터로 기록되면서, 디지털 포렌식은 범죄 수사에서 혐의를 밝히는데 중요한 역할을 하고 있다.

최근 대법원 판례에서는 디지털 증거에 대한 몇 가지 중요한 가이드라인을 제시하였다. 첫 번째는 저장매체 자체의 압수를 원칙적으로 금지한다는 것이다. 두 번째는 저장매체 또는 복제본을 수사 기관의 사무실 등으로 옮겨 이를 복제·탐색·출력하는 경우에도, 피압수자의 참여권을 보장하여야 한다는 것이다. 세 번째로 수사기관은 사건과 무관한 전자정보를 삭제 폐기해야 한다는 것이다. 대법원의 판결 취지를 반영하여 서울중앙지방법원은 “전자정보 압수수색 영장에 관한 새로운 실무 운영지침”을 시행하였다. 위 지침에 따르면 원칙적으로 전자정보를 압수대상으로 한다. 또한 압수한 전자정보는 상세 목록을 작성하여 피압수자에게 교부해야 하고, 범죄 혐의와 무관한 정보는 삭제·폐기하도록 하고 있다. 대법원 판례와 위 지침을 종합하여 살펴보면 범죄 혐의와 관련성 있는 정보만을 압수하고, 무관한 정보는 불가피하게 압수를 하였더라도 이를 삭제·폐기하라는 취지로 보인다.

위 대법원 판결에서 전자정보를 압수수색의 대상으로 판시함에 따라 디지털 증거의 특징을 고려한 관리방식이 필요하게 되었다. 디지털 증거는 진정성과 무결성 등의 요건을 갖춰야만 증거로서 사용될 수 있다. 디지털 증거의 무결성과 진정성을 보장하기 위해 디지털 데

이터를 획득할 때 Hash 값을 생성하여 검증하고, 디지털 증거를 법정에 제출할 때까지 서버에 통합 관리하는 등의 방법으로 보관의 연속성을 지킨다.

또한 디지털 증거의 대량성로 인하여 정보 획득에 긴 시간이 소요되거나 전문 인력에 의한 기술적 조치를 필요로 하는 등 여러 가지 문제에 봉착할 수 있다. 이러한 경우 현장에서 범죄사실과 관련된 데이터만을 출력·복제하는 방법으로 압수의 목적을 달성하기에는 무리가 있다. 결국 불가피하게 대량의 전자정보를 압수한 경우, 범죄혐의와 무관한 정보를 폐기해야 하는 문제가 남게 된다.

이에 검찰은 “압수대상으로서의 디지털 증거 관리 매뉴얼”을 시행하여, 압수한 전자정보를 디지털 수사망(D-NET)에 등록·처분하도록 하고 무체물인 전자정보를 관리하기 위한 방안을 마련하였다. 본 논문에서는 디지털 증거를 폐기하였거나 보관한 경우, 객관적·과학적으로 검증을 할 수 있는 방안을 제안하고자 한다. 블록체인을 이용하여 디지털 데이터의 로그를 관리하고 각각의 로그에 대한 해쉬 값으로 보관의 연속성을 입증하며, 폐기 시에는 폐기한 로그에 대한 해쉬 값과 블록체인에 저장된 해쉬 값을 비교하여 디지털 증거 관리에 이상 없음을 확인한다면 보다 효율적일 것이다.

블록체인을 활용한 디지털 증거 관리 방식은 보관·폐기의 확인 외에도 보관의 연속성을 보장하고, 사생활 보호 등에 대한 우려가 있는 자료가 어떻게 보관되었는지 확인해준다. 블록체인을 활용한 디지털 증거 관리 방식을 실무에서 적극적으로 사용하기 위해서는 기술적인 연구와 이를 뒷받침하는 관련 법리 등을 준비하는 것이 중요한 과제가 될 것이다. 본 논문이 디지털 증거 관리에 일조하여 실체적 진실의

발견을 위한 수사 · 공판에 도움이 될 뿐만 아니라, 피압수자의 기본권 보호에도 도움이 되는 합리적인 방법으로 활용되기를 기대한다.

주요어 : 디지털 증거 관리, 기밀 유출 방지, 블록체인
학 번 : 2015-26065

목 차

표 목 차

그 림 목 차

1. 서론

1.1. 연구의 배경

현대인에게 디지털 기기는 생활필수품이다. 사람들은 스마트폰으로 개인의 주요 관심사나 뉴스를 검색하고, 친구 또는 회사동료와 메시지를 주고받으며, 회사에서는 컴퓨터를 이용하여 보고서 등 문서를 작성·보관한다. 자동차를 운전할 때는 네비게이션과 블랙박스가 운전자의 위치 정보와 주변 상황 등을 기록하고, 곳곳에 설치된 CCTV는 거리를 지나가는 사람들의 움직임을 녹화한다. 또한 사물인터넷(IoT)의 사용으로 디지털 기기가 생활의 일부가 되면서, 생활 속에서 대부분의 행동들이 디지털 형태로 기록되고 있다. 디지털 시대가 도래함에 따라 디지털 정보의 양도 많아지고, 그 형태도 다양해졌다.

디지털 기기가 대중화됨에 따라 개인이나 기업의 중요한 정보가 디지털 형태로 저장되는 경우가 점점 늘어나면서, 개인이나 기업의 비밀 또는 범죄의 흔적을 담고 있는 경우도 증가하였다. 과거에는 범죄 수사에 아날로그 족적(발자국, 지문 등)들이 사건 해결의 실마리가 되었지만, 디지털화된 현대사회에서는 디지털 족적인 디지털 데이터를 활용하여 사건을 해결하는 경우가 많아지고 있다. 디지털 증거가 점점 중요해지고 있는 것이다. 최근에는 이러한 현실을 반영하여 형사소송법이 개정되었다. 디지털 포렌식의 발달로 인하여 사용자의 아이디, 비밀번호, 사용한 디지털 기기의 로그 기록, IP주소, 작성자의 위치정보 등 과학적이고 객관적인 방법을 통해 증거를 확보할 수 있는 길이 열린 것이다.

기술이 비약적으로 발전함에 따라 범죄행위에 사용되던 증거들도 종이 문서가 아닌 디지털 형태를 띠고 있다. 개정된 형사소송법에 따르면 피고인 또는 피고인 아닌 자가 작성하였거나 진술한 내용이 포함된 문자·사진·영상 등의 정보로서 컴퓨터용 디스크, 그밖에 이와 비슷한 정보저장매체에 저장된 것 등이 디지털 증거가 될 수 있다. 구체적으로 살펴보면 다음과 같다. 공판준비나 공판기일에서 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 경우에 증거로 할 수 있으며, 성립의 진정을 부인하는 경우에도 과학적 분석결과에 기초한 디지털 포렌식 자료, 감정 등 객관적 방법으로 성립의 진정함이 증명되는 때에는 증거로 할 수 있다. 다만, 피고인 아닌 자가 작성한 진술서는 피고인 또는 변호인이 공판준비 또는 공판기일에 그 기재 내용에 관하여 작성자를 신문할 수 있었을 것을 요한다. 피고인 아닌 자가 작성한 경우 반대신문권이 보장됨을 명확히 규정하려는 것이다.

형사소송법이 개정됨에 따라 유체물 중심으로 보관·처분하던 기존의 압수물 관리 규칙에서 무체물인 전자정보까지 압수 대상으로 하는 구체적인 방안의 필요성이 대두되고 있다. 유체물과는 다르게 디지털 증거는 진정성(동일성), 무결성 등을 고려하여 안전하게 관리해야 한다. 디지털 증거에 알맞은 안전한 관리 방안이 필요한 것이다.

1.2. 연구 목적

디지털 증거의 수집과 분석에 대한 논의는 활발하게 이루어지고 있는 반면에, 디지털 증거를 어떻게 관리할지에 대한 논의는 그렇지 못하다. 검찰과 경찰에서도 각각 “디지털 증거 수집 및 분석 규정”[1]을 둠으로써 디지털 증거의 수집 방법이나 분석시 유의해야할 점에 대해

정하고 있다. 하지만 압수한 디지털 증거를 어떻게 관리해야 할지에 대해서는 별도의 규정이 없다. 다행히 최근 대법원 판결[2]에서는 디지털 증거에 대한 몇 가지 중요한 가이드라인을 제시하였다. 첫 번째는 저장매체자체의 압수를 원칙적으로 금지한다는 것이다. 두 번째는 저장매체 또는 복제본을 수사기관 사무실 등으로 옮겨 이를 복제·탐색·출력하는 경우에도, 피압수자의 참여권을 보장하여야 한다는 것이다. 마지막으로 수사기관은 사건과 무관한 디지털 데이터를 삭제 폐기해야 한다는 것이다. 이로써 수사기관은 저장매체가 아닌 디지털 데이터를 원칙적으로 압수해야 하며, 사건과 관련 없는 데이터는 불가피하게 압수한 경우에는 삭제하여야 한다. 또한 디지털 데이터는 복제가 용이하여 디지털 정보가 수록된 저장매체 또는 데이터 복제본이 압수·수색 과정에서 외부로 반출되면 압수·수색이 종료한 후에도 복제본이 남아있을 가능성을 배제할 수 없다. 그 경우 혐의사실과 무관한 전자정보가 수사기관에 의해 다른 범죄의 수사 단서 내지 증거로 위법하게 사용되는 등 새로운 법익을 침해할 가능성이 있으므로, 혐의사실 관련성에 대한 구분 없이 이루어지는 복제·탐색·출력을 막는 절차적 조치가 요구된다. 이는 디지털 증거의 매체독립성, 변조가능성, 대량성 등과 같은 특징을 고려한 관리가 필요하며, 이러한 절차적 조치가 중요하다는 취지로 보인다.

실제로 압수·수색시 현장의 사정이나 디지털 데이터의 대량성으로 인하여 사건과 관련 있는 정보 획득에 긴 시간이 소요되거나 전문인력에 의한 기술적 조치가 필요한 경우에는 범위를 정하여 출력 또

---

1) 디지털 포렌식 수사관의 증거 수집 및 분석 규정, 대검찰청예규 제805호, 2015.7.16. 일부개정, 2015.7.16. 시행
디지털 증거 수집 및 처리 등에 관한 규칙, 경찰청훈령 제766호, 2015.5.22. 제정, 2015.6.1. 시행

2) 대법원 2015.7.16. 선고 2011모1839 전원합의체 결정

는 복제하는 방법만으로는 압수의 목적을 달성하기 어렵다. 또한 정보저장매체 자체 또는 하드카피 복제본을 압수하지 않고 범죄와 관련된 파일만을 압수하는 경우에는 삭제한 파일을 복구하기 어려우며, 메타데이터를 확보하지 못하여 세밀한 분석이 어렵다는 단점이 있다. 결국 사건에 따라서 어느 정도 포괄적인 압수가 불가피하고 이러한 경우 개인의 민감한 정보도 함께 혼재되어 압수될 수 있다. 디지털 데이터에는 개인정보와 같이 민감한 정보나 사건과 무관한 정보가 함께 담겨있는 경우도 있기 때문에 압수한 디지털 데이터를 어떻게 보관·폐기할지, 그리고 누구에게 열람하고 복제할 수 있는 권한을 부여할지 등의 실질적인 문제도 중요하게 다루어야 한다.

압수한 디지털 데이터에 대한 체계적인 관리 절차가 필요하며, 디지털 증거를 어떻게 관리할지에 대한 논의가 필요하다. 이 논문에서는 비트코인에서 활용되는 블록체인을 이용하여 디지털 데이터를 서버에 등록·열람·복제·폐기할 때 생성되는 로그들을 관리함으로써 디지털 증거에 대한 행위 이력을 안전하게 관리하고, 이러한 로그를 블록체인으로 연결함으로써 보관의 연속성이나 보관·폐기 등을 검증하는 방식을 제안하고자 한다. 이 논문에서 제안하는 방식은 디지털 증거의 관리뿐만 아니라 기업의 기밀 유출에 대비한 기업의 문서중앙관리서버에서 생성된 로그들을 관리하거나, 피압수자가 참관하지 않음을 동의한 경우에는 보조적인 방법으로 수사기관에서 사건과 관련된 자료를 복제하거나 관련 없는 증거를 폐기하였음을 확인하는데 활용할 수 있을 것이다.

1.3. 연구 방법

이 논문에서는 압수된 디지털 증거를 안전하게 관리하기 하기 위하여 블록체인과 비트코인이 어떻게 구성되어 있는지 검토하고, 이를 활용하여 디지털 데이터를 안전하게 관리하는데 적합한 방법을 제안하고자 한다.

블록체인과 비트코인을 살펴보기에 앞서 제2장에서는 압수물의 개념과 디지털 데이터가 압수의 대상인지 여부, 그리고 디지털 데이터의 특징과 디지털 증거의 요건 등에 대해 알아봄으로써 이에 대한 개념을 알아보도록 하겠다.

제3장에서는 압수한 디지털 데이터의 관리 및 처분상의 문제점에 대해서 검토해보고자 한다. 현행 검찰압수물사무규칙의 한계에 대해 검토해보고, 실무상 압수한 디지털 데이터를 등록·처분할 때 일어나는 현실적인 문제점과 이를 해결하기 위해 검찰에서 마련한 “압수대상으로서의 디지털 증거 관리 매뉴얼”을 살펴보겠다.

제4장에서는 디지털 데이터의 관리에 사용할 블록체인의 개념 및 구조에 대해 알아보겠다. 또한 비트코인의 개념과 비트코인 클라이언트의 유형 그리고 비트코인의 암호기술에 대해 살펴보고, 블록체인의 구조, 생성 방식, 종류와 해외 이용사례 등에 대해 알아보도록 하겠다.

제5장에서는 디지털 데이터를 관리하기 위해서 서버구성은 어떻게 할 것인지, 블록체인 중 어떤 방식을 채택하여 저장하고 검증할 것인지, 그리고 어떤 구조로 블록체인을 만들 것인지에 대해 생각해보고,

디지털 데이터 관리 방식을 제안하고자 한다.

대법원 판결에서 살펴본 바와 같이 기본권 보호 강화 움직임에 따라 혐의사실 관련성에 대한 구분 없이 이루어지는 복제·탐색·출력을 막는 절차적 조치가 중요하게 되었다. 이에 따라 검찰에서도 “압수대상으로서의 디지털 증거 관리 매뉴얼”을 시행하여 디지털 증거의 보관·폐기에 대한 절차를 마련하였다. 이 논문에서는 이와 더불어 디지털 증거의 행위 이력을 관리하여 구분 없이 이루어지는 열람·복제·탐색·출력을 감시하고, 이러한 이력의 유무를 객관적이고 과학적으로 증명할 수 있는 방안을 제안하고자 한다. 이 논문이 우리나라 수사기관의 디지털 증거 관리에 미약하나마 도움이 되기를 바란다.

2. 압수물의 개념

2.1. 압수물의 정의

압수란 물건의 점유를 취득하는 강제처분을 말하며, 압류와 영치 및 제출명령 세 가지를 내용으로 한다.[3] 압수물이란 수사기관이나 법령에 의하여 압수한 증거물, 몰수할 것으로 사료되는 물건(형사소송법 제106조 제1항), 우편물(형사소송법 제107조), 제출명령에 의하여 제출된 증거물, 몰수대상물(형사소송법 제106조 제2항) 또는 임의제출물, 유류물(형사소송법 제108조) 등을 말한다. 대부분의 압수는 증거물이나 몰수물을 대상으로 한다. 종래에는 유체물인 증거물 또는 몰수물만 압수의 목적물로 보았으나 형사소송법의 개정으로 정보저장매체의 압수를 명문으로 규정함으로써 이를 해결하였다.[4] 즉, 무체물인 디지털 데이터에 대한 압수를 인정한 것이다.

2.2. 디지털 데이터와 증거의 개념

2.2.1. 디지털 데이터의 의의

디지털(digital)이란 "아날로그에 대응되는 개념으로 자료를 연속적인 실수가 아닌, 특정한 최소 단위를 갖는 이산(離散)적인 수치를 이용하여 처리하는 방법"[5]을 말한다. 디지털 데이터란 정보저장매체에 저장되어 있거나 네트워크를 이용하여 전송 중인 전자정보로, 0과

3) 이재상, 조균석, 형사소송법, 박영사, (2015)
4) 이재상, 조균석, 형사소송법, 박영사, (2015)
5) <https://ko.wikipedia.org/wiki/디지털> 2016.11.14. 최종검색

1의 2진법 논리로 표현되는 데이터를 의미한다. 전기적 신호를 0과 1의 조합으로 디지털기기의 저장과 처리를 통하여 정보를 만들거나, 그 정보를 송·수신하게 할 수 있다. 0 또는 1로 표현되는 디지털 데이터의 최소 단위는 비트(bit)이며, 이는 2진법 또는 16진법 수 체계 표현에 적합하다.

2.2.2. 디지털 데이터의 특징

디지털 데이터는 매체독립성, 비가시성·비가독성, 변조 가능성·복제 용이성, 휘발성, 대량성, 초국경성 등 유체물과 다른 특징을 지닌다.

디지털 데이터는 매체의 형태와 무관하게 독립하여 존재한다. 따라서 어떠한 저장매체에 저장되어 있든지 동일한 데이터는 동일한 가치를 지닌다. 또한 원본과 사본 구별이 불가능하다. 이러한 특성으로 인하여 범죄자는 데이터를 무한 복제하여 범죄에 악용할 수 있고, 반대로 수사관은 원본의 훼손을 막기 위해 사본을 만들어 데이터를 분석함으로써 무결성을 보장 할 수 있다. 또한 회사의 서버 또는 컴퓨터에 저장된 데이터를 압수할 경우 정보저장매체 자체를 압수하는 것은 긴 시간이 소요되거나 전문 기술자의 조치를 필요로 하는 등의 어려움도 있지만, 해당 회사의 영업활동에 불편을 초래할 수 있다. 이러한 이유로 저장매체를 압수하는 대신 저장매체에 담겨있는 디지털 데이터만을 복제하고 검증한 후 이를 압수하는 것이 일반적인데, 이는 매체와 독립한 디지털 데이터의 특성에서 기인한 것이다.

디지털 데이터는 실제로는 0과 1인 이진수의 형태로 정보저장매체에 저장되어 있기 때문에 사람의 눈으로는 읽을 수 없다. 따라서 디지

털 데이터의 실제 내용을 확인하기 위해서는 그에 맞는 전용 뷰어인 소프트웨어와 모니터나 프린터 같은 출력 장치가 필요하다. 비가시성과 비가독성으로 인해 범죄행위와 관련된 디지털 데이터를 스캔할 때에는 그에 맞는 수사 장비가 필요하다.

디지털 데이터 내부에 존재하는 0과 1의 전자 정보는 쉽게 위·변조가 가능하고, RAM과 같은 휘발성 저장매체에 저장된 데이터나 네트워크에서 사용되는 패킷은 시스템 환경의 변화로 인하여 쉽게 사라질 수 있다. 이와 같이 디지털 데이터는 쉽게 변하거나 사라지며, 이러한 사실을 찾아내는 것이 쉽지 않기 때문에 법정에서 조작여부, 증거획득 절차 등의 적정성 문제가 제기되기도 한다. 현재 디지털 포렌식 실무에서는 압수·수색시에 디지털 데이터를 복제하고 Hash 값을 만들어 검증하는 방식으로 디지털 데이터의 무결성을 보장하고 있다.

디지털 데이터는 그 양이 방대하여 특별한 기술과 도구, 교육된 전문 인력을 사용하지 않고서는 증거 추출이 곤란하다. 기업의 전산·회계자료, 데이터베이스 같이 양이 방대한 자료가 그렇다. 또한 큰 용량의 저장매체들이 보편화 되어 개인이 소지하는 데이터의 양도 증가하였다. 이러한 특성 때문에 압수·수색시 사건과 관련된 자료만을 선별하여 압수하는 것은 점점 어려워지고 있다.

디지털 데이터는 네트워크를 통해 장소적 제한을 받지 않고 원거리에 존재하는 서버나 컴퓨터에도 존재할 수 있다. 구글이나 텔레그램과 같은 해외의 인터넷, 클라우드, 메신저 서비스를 사용하면 데이터의 저장 위치가 국경을 초월하여 존재한다. 이러한 특성 때문에 증거확보 과정에서 해외에 저장 되어있는 디지털 데이터를 수집하는 경우, 국제공조와 관할권에 대한 문제가 발생할 수 있다.

2.2.3. 디지털 증거의 의의

아직까지 디지털 증거에 대하여는 그 개념이 정확하게 정립되지 않은 것으로 보인다. 1995년에 창설된 IOCE는 디지털증거에 대해서 “이진수 형태로 저장 혹은 전송되는 것으로 법정에서 신뢰할 수 있는 정보”[6]라고 정의하였고 1998년에 SWGDE에서는 디지털 증거에 대해 “디지털 형태로 저장되거나 전송되는 증거가치가 있는 정보”[7] 라고 정의하였다. E.Casey에 따르면 디지털 증거(Digital evidence or Electrinic evidence)는 “디지털 형태로 저장되어 있거나 네트워크를 통해 전송 중인 자료로서 법정에서 신뢰할 수 있으며 증거 가치가 있는 정보”[8] 라고 한다. 디지털 증거는 일반 증거와 구별되는 요건들이 있다. 이러한 요건들을 다음에서 살펴보겠다.

2.2.4. 디지털 증거의 요건

디지털 증거는 디지털 형태로 저장되거나 전송되는 증거가치 있는 정보로서 0과 1의 이진수 방식으로 존재하고, 정보저장매체와 별개의 무체의 정보이며, 증거로서의 가치를 가진 정보이다. 디지털 데이터가 법정에서 증거로 사용되기 위해서는 기본적으로 갖추어야 할 몇 가지 요건이 있다.

첫 번째로 디지털 증거수집 절차의 진정성이다. 법정에 제출된 증거는 혐의사실을 증명하기 위해 수집한 증거와 동일하여야 한다. 디지털 증거의 저장, 수집 과정에서 오류가 없고, 압수하고자 하는 데이

6) IOCE(International Organization on Computer Evidence)의 정의
7) SWGDE(Scientific Working Group on Digital Evidence)의 정의
8) Eoghan Casey, Digital Evidence and Computer Crime, (2011)

터가 정확히 수집되었고, 그로 인해 생성된 자료임이 인정되는 것을 뜻한다. 그러기 위해서는 압수ㆍ수색 시점부터 법정에 제출된 단계까지 모든 과정에서 보관의 연속성(Chain of Custody)이 보장되어야 한다.

그 다음은 디지털 증거 데이터의 무결성이다. 디지털 증거는 증거 취득 시점부터 법원에 증거로 제출할 때까지 부당한 수정, 변경, 손상이 없어야 한다. 이를 위해서는 데이터를 특정 시점의 상태로 고정시키고, 삭제 파일이나 빈 공간까지 비트 단위로 복제하여 저장하는 이미징 작업이 필수적이다. 또한 이미징 작업을 한 이후에 데이터의 변경을 방지하고자, 이미지 파일에 대한 고유 번호(32자, 128bit의 16진법 숫자 조합)를 생성하여 1 bit라도 손상되면 그 고유 번호가 변경되도록 해쉬 값을 부여하는 방식으로 무결성을 보장한다.

마지막으로 디지털 증거수집 방식의 신뢰성이다. 디지털증거의 수집 분석과정에서는 의도하지 않은 오류가 발생하지 않도록 증거수집 도구의 신뢰성이 요구되며, 증거를 분석하고 취급하는 자의 전문성 또한 요구된다.

디지털 증거는 유체물인 증거와는 다르게 법정에서 의미 있는 증거로 사용되기 위해서는 위와 같은 요건들을 갖춰야하며, 위의 요건들을 갖추지 못한 경우에는 증거로서 인정을 받을 수 없게 된다.[9] 따라서 위의 요건들을 충족하는 상태로 디지털 증거를 유지시켜 주는 관리 시스템이 필요하다.

9) 장상귀, 디지털 증거의 증거능력에 관한 연구, 법학실무연구회 (2009)

3. 압수한 디지털 데이터의 관리 및 처분상 문제점

3.1. 현행 검찰압수물사무규칙의 한계

검찰압수물사무규칙은 압수물을 수리하여 처분할 때까지의 사무에 관한 사항을 정하고, 압수물 사무의 적정한 운영을 기하기 위해 마련된 규칙이다. 현행 압수물사무규칙은 유체물인 압수물을 대상으로 하는 규칙으로써 디지털 데이터의 관리 및 처분에 적용하기에는 다소 무리가 있다.

형사소송법은 압수의 목적물이 컴퓨터에 저장된 전자정보인 경우, 범위를 정하여 출력 또는 복제하거나 이러한 방법이 불가능한 경우 정보 저장매체 자체를 압수할 수 있다고 정하고 있다. 하지만 검찰압수물사무규칙에서는 유체물인 컴퓨터 등 전자저장매체에 대해서는 일반 압수물로 취급하고 있지만, 디지털 데이터 혹은 전자 정보라는 개념은 다루지 않고 있다. 검찰압수물사무규칙 제2조 1호는 압수물에 대해 이렇게 정의한다. “압수물이라 함은 압수된 물건과 환가대금 및 통신제한조치 집행으로 취득한 물건을 말한다.” 위 규칙은 디지털 데이터 또는 전자정보라는 개념을 다루고 있지 않기 때문에, 이의 등록 또는 처분 시 적용할 수 있는 규정의 부재로 관리에 어려움이 있다. 구체적인 내용을 살펴보면 다음과 같다.

검찰압수물사무규칙 제4조 제2항에서는 “압수물사무담당직원은 압수물과 사건기록의 압수물 총목록 및 압수조서 등을 대조 확인하여 이를 수리하여야 한다.” 고 규정하고 있다. 하지만 무체물인 디지털 데이터는 그 특징상 유관으로는 볼 수 없기 때문에, 사건과 관련성을 나

타내기 위해서는 설명이 필요하며, 특정한 도구를 사용하지 않으면 내용을 확인하기 어렵다. 또한 압수하거나 임의 제출한 디지털 기기의 데이터들을 논리이미지 형태로 가져오기 때문에 데이터의 무결성을 증명하는데 쓰이는 해쉬 값이 변하지 않도록 데이터를 안전한 곳에서 보관하여야 하고, 사건 담당자가 아닌 자(또는 권한 없는 자)의 열람 · 수정 · 복제 · 삭제를 금지하는 등의 관리가 필요하다. 또한 압수한 디지털 데이터를 사건 처분 후에도 계속 보관 결정할 경우, 그 보관기간을 정해야 하는데 위 규칙에는 이에 대한 부분이 마련되어 있지 않다.

헌법재판소는 “압수의 궁극적인 목적은 증거물 또는 몰수대상물을 수집, 보전하여 장차 공판절차에서 증거물로 이용하거나 이를 몰수하고자 하는 데 있으므로, 압수물은 재판의 확정시까지 압수 당시의 성질, 상태, 형상을 그대로 보전 · 유지하여 보관할 필요성이 있다. 또한 압수물의 보존이 형사소송법절차에 있어서 검사의 입증 편의만을 위한 것만은 아니다. 형사소송절차에서는 피고인에게도 자신에게 유리한 사실을 입증하기 위한 증거신청권이 있고, 압수물은 공소사실의 입증뿐만 아니라 피고인에게도 유리한 자료(반증 및 양형 자료 등)로 사용될 수 있는 것이므로, 피고인의 입장에서 압수물의 증거 조사를 통하여 자신에게 유리한 사정을 입증하고자 하여도 압수물이 폐기되어 존재하지 않게 된다면 이는 증거 신청권을 포함하는 피고인의 공정한 재판을 받을 권리를 침해하게 된다.” 라고 판시하여, 일반적으로 압수물은 해당 사건이 종결될 때까지 보존함이 원칙이라고 본다.[10] 예외적으로 수사절차나 소송절차가 종료하기 전에라도 처분이 필요한 경우가 있고, 위험발생의 염려가 있는 압수물이나 부패의 염려가 있거나 보관하기 어려운 압수물은 소유자 등 권한 있는 자의 동

10) 헌법재판소 2012.12.27. 선고 2011헌마351 결정

의를 받아 폐기하는 경우도 있지만, 이러한 경우는 논문에서 다루지 않도록 하겠다. 헌법재판소는 동 결정에서 일반적으로 압수물은 증거물로써 더 이상 가치가 없을 때까지 보관하는 것이 공정한 재판의 실현을 위해 필요하다는 입장을 밝혔다. 압수의 대상이 되는 디지털 데이터도 예외일 수는 없기 때문에 이러한 내용들을 검찰압수물사무규칙에 반영하여 보완하여야 하겠다. 이하에서는 위 규칙의 한계점을 보완하기 위해 검찰에서 시행한 매뉴얼을 살펴보겠다.

3.2. 실무상 압수한 디지털 데이터의 등록 및 처분

검찰에서는 압수수색 과정에서 복제하여 확보한 디지털 데이터를 디지털 수사망(이하 D-NET)[11]에 통합 관리하고 있다. 개정 형사소송법에서 전자정보를 압수의 대상으로 인정하였고, 이의 압수방법에 대해서는 출력이나 복제를 원칙으로 하고, 예외적으로는 정보저장매체 자체를 압수하도록 규정하였다. 이에 따라 현장에서 정보저장매체 자체를 압수하여 수사기관으로 가져와 물리적 이미징을 한 후, 이 이미지 파일을 분석하고 결과를 보고하던 방식에서, 압수ㆍ수색 현장에서 사건과 관련된 디지털 데이터를 논리 이미지로 복제하는 것을 원칙으로 하고, 예외적으로 저장매체를 압수하는 방식으로 바뀌게 되었다. 또한 대용량 저장매체 보급과 모든 문서의 디지털화 등으로 인하여 기업에서는 서버를 구축하여 대용량 자료를 관리하거나, 기업의 기밀 유출 방지를 위해서 DRM, 파일 암호화, PC 가상화 등의 기술을 사용하면서 기존의 방식으로는 증거 획득이나 분석이 어려워졌다. 이

11) D-NET은 검찰의 디지털수사팀을 온라인으로 연계하여 신속한 수사 지원 시스템을 제공하고, 디지털증거분석 업무의 편의성 및 증거 관리의 엄격성을 향상시키기 위한 선진 디지털수사 네트워크로서 2011. 3.부터 사용하고 있다.

러한 수사 환경으로 인하여 검찰에서는 디지털 증거를 하나로 통합하여 관리 · 분석하기 위한 디지털 증거 관리 시스템을 구축하게 되었다.

또한 검찰에서는 최근 대법원 판례와 서울중앙지방법원 실무지침의 영향으로 “압수대상으로서의 디지털 증거 관리 매뉴얼”[12]을 시행하였다. 이 매뉴얼은 “디지털 포렌식 수사관의 증거수집 및 분석 규정”상 디지털 수사 지원 절차를 통해 압수되거나 증거분석 의뢰되어 D-NET에 보관중인 디지털 증거를 관리함을 목적으로 한다. 이하에서는 검찰이 마련한 압수물 등록 · 처분 절차를 살펴보겠다.

3.2.1. 압수물의 등록

위 매뉴얼에서는 압수물을 등록하는 절차를 ① 압수물 수리 준비 ➜ ② 등록 대상 디지털 증거 선정 ➜ ③ 압수조서 및 압수물총목록 작성 ➜ ④ 압수물의 수리의 4단계로 나누고 있는데, 자세한 내용은 다음과 같다.

압수물 등록을 위해서는 먼저 압수물 수리 준비 과정을 거쳐야 한다. 검찰은 압수 · 수색이나 임의제출 등의 방법으로 디지털 데이터를 획득할 때 압수 대상자에게 “수사 또는 재판 목적 소멸시 전자정보 폐기 예정 사실”을 고지하고 동의서에 확인을 받도록 하고 있다.

그 다음 수사팀에서 등록 대상인 디지털 증거를 선정한다. 선정하는 과정에서 압수하였거나 임의제출 받은 자료가 범죄사실과의 관련성이 인정되지 않는 등으로 인하여 보관이 불필요한 경우, 수사팀에

12) 대검찰청, 압수대상으로서의 디지털 증거 관리 매뉴얼 (2016)

서는 폐기 요청을 할 수 있다. 이러한 경우에는 압수물 등록 절차 없이 폐기한다. 등록 대상으로 확인된 디지털 증거에 대해서는 반드시 압수조서, 압수물총목록 등을 작성한다.

세 번째 단계는 압수조서 및 압수물총목록 작성이다. 디지털 수사지원을 통해 디지털 증거를 확보한 수사팀에서는 디지털 증거의 압수물 수리에 필요한 디지털 증거 보관 확인서, 압수 조서, 압수물총목록을 작성한다. 디지털 증거 보관 확인서는 D-NET에 압수물이 잘 보관되어 있음을 확인하기 위한 것으로써 위 매뉴얼을 통해 새롭게 도입되었다. 디지털 증거 보관 확인서에는 사건번호, 지원번호, 디지털 증거명, 용량, 등록 일시, 담당 포렌식 수사관, 보관 증거번호 등을 기재하고 하단에 수사검사가 서명한다.

마지막 네 번째 단계는 압수물의 수리이다. 압수물 관리 담당부서에서는 수사팀에서 작성한 디지털 증거 보관 확인서, 압수조서, 압수물총목록을 확인하고 KICS 압수물 관리 시스템에 디지털 증거를 압수물을 등록하여 수리한다.

3.2.2. 압수물의 처분

위 매뉴얼에 따르면 압수물의 처분은 ① 디지털 증거에 대한 폐기 지휘, ② 디지털 증거에 대한 폐기 촉탁 이렇게 2단계로 이루어진다. 사건을 처분할 때 수사검사는 계속 보관의 필요성이 없는 디지털 증거에 대해 폐기(촉탁) 지휘한다. 그 다음 검찰사건사무규칙에 따라 기소시에는 압수물건처분서에 그 내용을 기재하고, 불기소시에는 불기소결정서에 압수물에 대한 처분 명령을 기재한다. 또한 재판 확정

시에도 일선 청 압수물 담당 검사는 폐기(촉탁) 지휘를 하여야 한다. 판결에서 몰수선고를 하지 않았을 경우에는 원칙적으로 제출인에게 환부(형사소송법 제134조, 준용규정 제219조, 제332조)해야 하나, D-NET에서 보관 중인 디지털 증거의 경우 재산적 가치가 없는 복제된 전자정보(사본)이며 피압수자 등에게 “수사 또는 재판 목적 소멸 시 전자정보 폐기 예정” 임을 사전에 고지하였으므로 보관 목적이 없어진 압수한 디지털 증거는 폐기(촉탁)의 방법으로 처분하도록 하고 있다.

다음으로 디지털 증거에 대한 폐기 촉탁이 승인되면, 압수물 관리 담당 부서에서는 디지털수사통합업무관리시스템(DFIS Ⅱ)에 접속하여, 사건번호나 지원번호 등으로 폐기 대상인 압수물의 사건을 검색한 후 폐기 촉탁을 요청한다. 디지털 증거 폐기 촉탁 요청을 받은 국가디지털포렌식센터(이하 NDFC)에서는 디지털 증거를 폐기하고 이에 대한 회보를 압수물 관리 담당 부서에 보내고, 압수물 관리 담당 부서에서는 디지털 증거 폐기 확인서를 인쇄하여 보관한다.

일련의 절차를 살펴보면 그림 1[13]과 같다. 압수한 디지털 데이터를 등록 대상으로 선정하고 처분할 때까지 수사팀과, 압수물 관리 담당부서 그리고 NDFC가 협업하여 관리한다. 검찰은 압수한 디지털 데이터를 D-NET에 통합하여 관리하고 있으며, 위 매뉴얼에서는 디지털 데이터를 압수의 대상으로 보고 실무상 검찰압수물사무규칙에서 다루지 못한 부분을 보완하고 있다.

13) 대검찰청, 압수대상으로서의 디지털 증거 관리 매뉴얼 (2016)

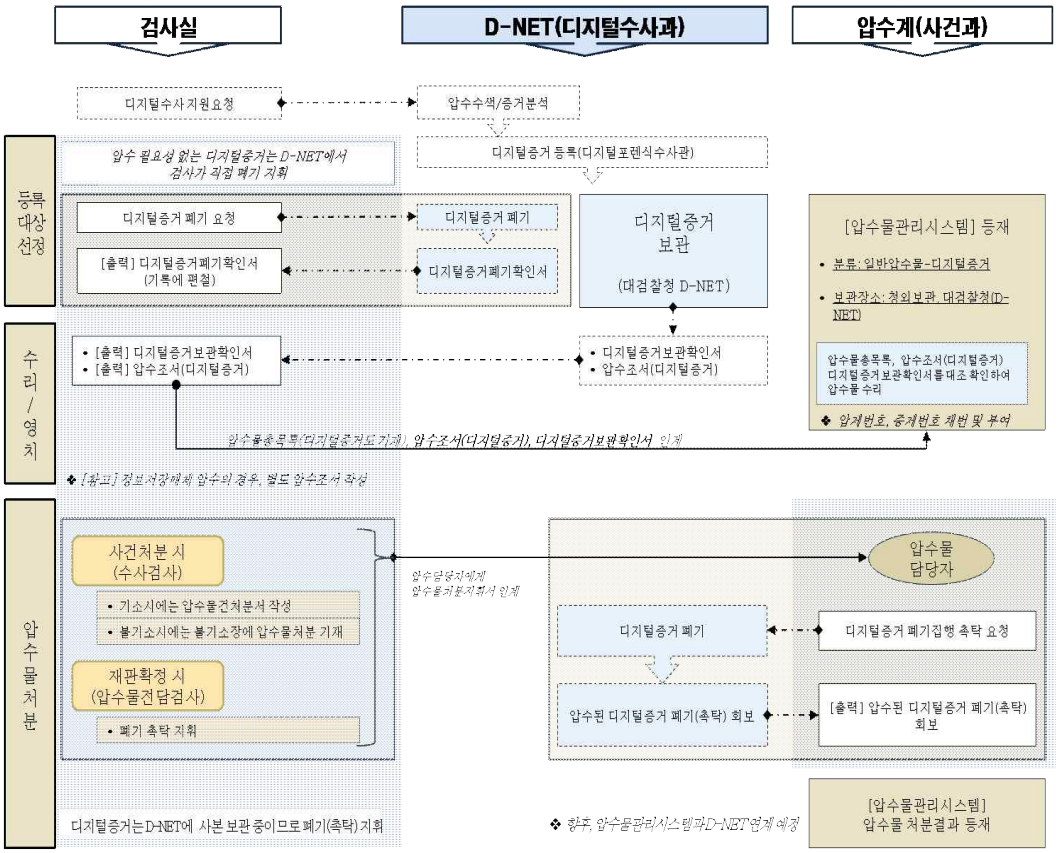


그림 1 압수대상 디지털 증거 관리절차

또한 위 매뉴얼은 디지털 증거의 관리 방법뿐만 아니라 디지털 증거를 계속 보관할 경우 그것의 보관기간에 대해서도 디지털 데이터의 획득 시 압수대상자에게 “수사 또는 재판 목적 소멸 시 전자정보 폐기 예정 사실”을 고지하고 동의서를 받음으로써 해결하였다. 다만 아쉬운 점이 있다면, 디지털 증거를 보관하고 폐기하였다는 확인서에 대해서 객관적인 증명이 부족하다는 것이다. 보관 또는 폐기에 대한 객관적인 증명에 대해서는 뒤에서 기술하기로 한다.

4. 비트코인과 블록체인의 개념

앞서 언급한 바와 같이 현재 검찰에서는 D-NET을 통해 압수한 디지털 데이터를 보관하고 있지만, 실무에서 필요한 디지털 증거를 보관하고 폐기하였다는 확인서를 어떻게 증명할지는 해결되지 않았다. 몰수 선고 또는 수사 · 재판의 목적 소멸 시 압수한 디지털 데이터를 폐기하였음을 과학적으로 증명할 수 있고, 추가적으로 몇 가지 사항이 준비된다면 참관을 희망하지 않는 상황에서는 피압수자의 참관이 없어도 관련 자료를 열람 · 출력 · 복제 · 삭제하였음을 보여주는 행위 이력을 블록체인을 활용하여 과학적이고, 객관적으로 확인할 수도 있을 것이다. 블록체인은 비트코인 거래 정보의 보안을 위해 만들어졌기 때문에 블록체인을 살펴보기에 앞서 비트코인에 대해서 알아볼 필요가 있다. 이하에서는 비트코인에 대해 알아보고자 한다.

4.1. 비트코인의 개념

4.1.1. 비트코인의 의의

비트코인은 2008년 “나카모토 사토시”가 발표한 논문을 바탕으로 개발된 전자 화폐이다. 비트코인은 금융기관을 제3자 신용기관(Trusted Third Parties)으로 하는 기존의 방식과는 다르게 이를 발행하고 관리하는 중앙 기관의 개입 없이 분산된 형태의 전자적 P2P(Peer-to-Peer) 지급 구조를 가지고 있다. 즉, 비트코인은 그림 2[14]와 같이 중앙 서버 없이 거래정보를 블록체인(BlockChain) 형태

14) <DUPress.com, Deloitte University Press> 2016.11.14. 최종검색

로 저장하여 거래의 최종 승인 등을 네트워크 참여자들이 공동으로 수행한다. 거래의 시간 순서에 따라 네트워크 참여자들이 공동으로 거래를 입증하게 만들도록 하는 “P2P 분산 네트워크” 를 기반으로 중앙 서버 없이 거래를 보호할 수 있다.

또한 비트코인은 공개키 암호 방식[15]을 이용해 공개된 계정 간에 거래를 하며, 분산된 시간서버로 일련의 작업증명(proof-of-work)을 하여 중복지출(double-spending)을 방지한다.[16] 신규 화폐는 채굴(Mining)[17]에 의해 발행되며, 동시에 새로운 블록이 생성된다.

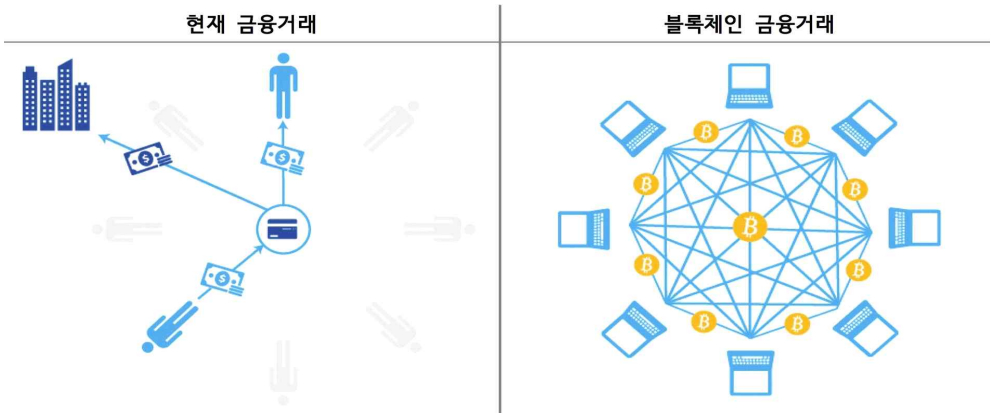


그림 2 기존 금융거래와 블록체인 금융거래의 비교

15) 암호 방식의 한 종류로 사전에 비밀키를 나눠가지지 않은 사용자들이 안전하게 통신할 수 있도록 한다. 공개키 암호 방식에서는 공개키와 비밀키가 존재하며, 공개키는 누구나 알 수 있지만 그에 대응하는 비밀키는 키의 소유자만이 알 수 있어야 한다. 공개키 암호를 구성하는 알고리즘은 대칭키 암호 방식과 비교하여 비대칭 암호라고 부르기도 한다.
<https://ko.wikipedia.org/wiki/공개_키_암호_방식> 2016.11.14. 최종검색

16) <https://ko.wikipedia.org/wiki/비트코인> 2016.11.14. 최종검색

17) 채굴이란 거래의 유효성을 검증하는 과정으로, 특정 조건을 만족하는 넌스(Nonce)를 찾아 블록을 생성하는 참여자에게 보상하는 개념으로 작업증명(Proof of work)이라고도 함

4.1.2. 비트코인 클라이언트 유형

4.1.2.1. Full Clients

풀 클라이언트는 전체 비트코인 프로토콜을 구현할 수 있고, 모든 비트코인 거래 참여자가 거래한 비트코인 정보를 가지고 있는 블록체인의 복사본을 저장한다. 전체 블록체인의 복사본은 수신한 모든 거래내역[18]을 검증하고 그것들이 합법적인 거래인 경우 모든 비트코인 거래 참여자들에게 방송한다. 풀 클라이언트에서는 비트코인 거래 참여자들이 직접 지갑을 관리하며, 비트코인 네트워크에서 직접 거래를 만들어 낼 수 있다.

하지만 풀 클라이언트를 사용하면 몇 가지 단점이 있다. 그 중 하나는 과도한 저장 공간의 사용이다. 풀 클라이언트는 전체 블록체인 복사본을 가지고 있기 때문에 기본적으로 사용하는 용량이 크며, 전체 블록체인 복사본의 크기는 거래가 늘어날수록 점점 더 커질 것이다. 또 하나의 단점은 과도한 양의 네트워크 대역폭 사용이다. 풀 클라이언트는 모든 거래내역을 항상 모니터링하고 있기 때문에 거래내역이나 블록을 송수신함에 오랜 시간이 걸린다. 그럼에도 불구하고 풀 클라이언트는 전체의 블록체인을 보관하고 있기 때문에 비트코인 네트워크의 보안성을 높여주고, 해커 등의 외부 공격으로부터 보호해 준다는 장점도 있다.

4.1.2.2. Headers-only Clients

18) 거래내역이란 고유한 식별번호인 비트코인 주소들 사이의 연결 · 흐름만을 의미하고, 거래와 연계된 이용자의 개인정보는 현출되지 않는 특유의 익명성을 가진다.

풀 클라이언트를 사용하여 전체 블록체인 데이터를 저장한다면, 저장 공간이 작은 스마트폰 같은 디지털 기기에서는 이용하기 어렵다. 이런 비트코인 거래 참여자들을 위한 클라이언트가 바로 Headers-only clients 이다. 이것은 전체 블록체인을 저장하지 않고 블록체인의 헤더만 저장한다. Headers-only clients는 비트코인 거래 참여자의 지갑을 관리하지만, 제3자가 소유한 서버에 의존하여 비트코인의 거래내역을 송수신 한다. Headers-only clients는 거래내역이 상정되었을 때, 또는 지갑 안에 있는 블록체인을 검색하여 거래를 검증하기 위해 가끔 전체 블록을 다운로드한다. Headers-only clients는 전체 블록체인에 대한 거래내역을 확인할 수 없는 경우라고 하더라도 몇 가지 환경이 갖추어 진다면, 풀 클라이언트만큼 안전해질 수 있다.

Headers-only clients는 전체 블록뿐만 아니라 거래내역과 해당 해쉬 트리들을 다운로드하지 않고 블록의 거래내역을 증명한다. 따라서 거래 검증을 위해서는 제3자 서버에 의존해야 하며, 이것으로 거래내역 전부에 대한 복사본 없이도 어떤 거래내역이 특정 블록에 포함된 것을 확인하기에 충분하다. 풀 클라이언트와는 다르게 네트워크 대역폭을 많이 절약한다.

4.1.2.3. Singing-only Clients

Singing-only Clients는 거래에 서명은 하지만, 블록체인 또는 블록헤더에 처리하지 않는다. 대신, Singing-only Clients는 서버에서 특정 거래내역에 관한 데이터를 요구한다. 만약 비트코인 네트워크에 연결된 비트코인 거래 참여자에게 거래가 생기면 이러한 거래내역이 지갑에 포함되며, 서버도 그 거래내역에 관심을 갖고 특정 참여자에

게 이러한 정보를 보낼 수 있다. Singing- only Clients는 자신의 거래내역과 키만을 저장하고, 비트코인 거래 참여자와 관련된 거래내역만을 전송하기 때문에 Singing-only Clients의 오버헤드[19]는 풀 클라이언트나 Headers-only clients보다 낮다. 따라서 저장 공간(Storage)은 오직 본인의 키와 거래내역에 대해서만 사용되고, 참여자와 관련된 거래내역만을 주고받는다. Singing-only Clients의 장점은 적은 저장 공간과 적은 네트워크 대역폭 및 컴퓨팅 파워를 사용한다는 것이다. 따라서 PC 응용 프로그램이나 모바일 애플리케이션 또는 웹 애플리케이션 등 다양한 방법으로 구현될 수 있다. 웹 기반의 서명 전용 클라이언트에서 암호화 기능은 자바스크립트로 구현되어 있으며, 웹 브라우저에서 실행되기 때문에 지갑의 비밀 키는 암호화된 서버로만 전송된다.

Singing-only Clients의 서버는 비트코인 거래 참여자의 모든 거래내역을 알 수 있기 때문에 높은 수준의 신뢰도가 요구된다. 서버 운영자가 이를 악용하여 잘못된 거래 내역을 보내 참여자가 실제로 가진 비트코인의 양을 속이는 공격을 할 수도 있지만 이러한 공격은 그다지 위험하지는 않다. 왜냐하면 그들이 참여자의 의사에 반하여 서명 거래 내역을 속일 수 없기 때문이다. 또한 서버 운영자의 입장에서도 유익하지도 않기 때문에 이러한 공격은 사실상 무의미 하다. 또한 이러한 방식의 공격은 오픈 소스 소프트웨어를 설정하는 여러 서버나 참여자의 서버에 연결함으로써 완화할 수 있다.

4.1.2.4. Thin Clients

Thin clients는 개인키를 보유하고 있지 않으며 거래에 서명하지 않

19) OS가 시스템을 관리하는데 필요로 하는 CPU 타임이나 메모리용량

는다. 대신 이러한 작업을 수행하기 위해 원격 서버에 명령을 보낸다. 원격 서버가 은행의 역할을 하게 되며, 비트코인 거래 참여자에게 금융 서비스를 제공한다. 전적으로 제3의 서버에 의존하는 Thin clients의 가장 큰 장점은 비트코인 거래 참여자가 이러한 작업이 서버에서 실행될 수 있게끔 개인키를 백업하게 되면, 이것을 안전하게 유지해야 한다는 문제를 간단하게 해결할 수 있다. 그러나 편리한 만큼 보안상으로는 위험하기 때문에 단점으로도 작용한다.

4.1.3. 비트코인 암호기술

비트코인은 공개키 암호 방식[20]과 해쉬 암호 방식[21]을 이용한다. 공개키 암호 방식은 거래내역이 변경되지 않았음을 입증하고, 거래의 익명성을 보장하는데 이용된다. 비트코인을 거래할 때 생성되는 거래내역의 무결성을 검증하기 위해서 거래내역을 해쉬하고, 거래내역의 해쉬값을 비트코인 거래 참여자의 개인키로 서명하여 상대방에게 보낸다. 수신자는 비트코인 거래 참여자의 공개키로 복호화 함으로써 전자서명을 검증하여 거래내역이 변경되지 않았음을 확인한다. 일련의 과정을 보면 그림 3[22]과 같다.

비트코인 거래 참여자의 공개키는 참여자 자신의 주소로 사용된다. 따라서 비트코인 거래 참여자 간에 거래 금액이 얼마인지는 알 수 있으나, 공개키에는 참여자의 정보를 포함하고 있지 않기 때문에 비트코인 거래의 익명성이 보장된다.

---

20) 대표적인 공개키 암호 방식으로는 RSA, ECDSA가 있다.
21) 해쉬 함수를 통해 해쉬 값으로부터 원래의 입력 값과의 관계를 찾기 어려운 성질을 가지지는 암호 방식으로 해쉬함수의 종류로는 MD5, SHA 계열이 있다.
22) 금융보안원, 블록체인 및 비트코인 보안 기술 (2015)

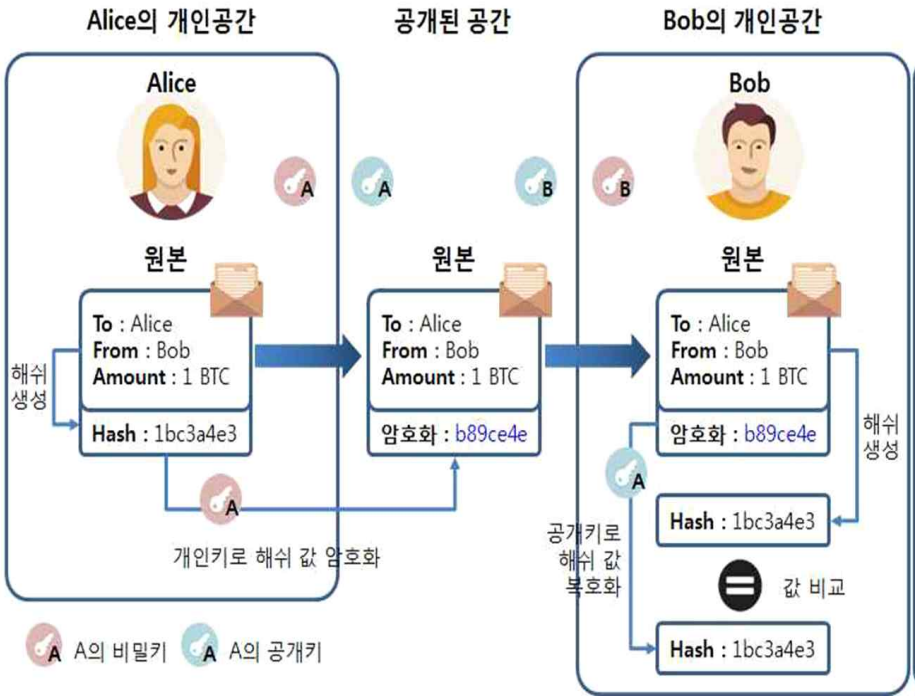


그림 3 비트코인에서 디지털 서명

해쉬 암호 방식은 채굴(mining)과 거래내역 입증 간소화에 주로 이용된다. 채굴에 대해서는 앞에서 언급하였으므로 생략하고, 여기서는 거래내역 입증 간소화에 대해 설명하겠다. 거래내역 입증을 위해서 각각의 거래 내역의 해쉬 값을 누적하는 해쉬 트리 구조를 이용한다. 해쉬 트리의 루트 값만 가지고 있어도 중간에 어떤 값이 변경될 경우 루트 값이 변경되어 전체 거래내역의 변조 여부를 쉽게 확인할 수 있다. 해쉬 트리는 머클 트리(Merkle tree)라고도 하는데, 주로 규모가 큰 데이터 집합을 효율적으로 요약하고 검증하는데 사용하는 데이터 구조다. 해쉬 함수를 이용하여 블록의 바디(Body)에 있는 모든 거래내역를 요약하고, 이를 루트(혹은 해쉬 루트)라고 부르는 해쉬 값 하나만 남을 때까지 두 개의 해쉬 값들을 다시 해쉬하여 트리 구조로 모든 거래내역을 관리한다. 해쉬 트리는 특정 거래내역이 블록 내부에 포함되어 있는지 검증하는데 매우 효율적이다.

데이터를 검증하고자 하는 사용자는 루트의 해쉬 값만 알면 데이터가 옳은 데이터인지 검증할 수 있다. 또한 데이터 전체가 아닌 일부만 검증하고자 할 때에도 자식 노드 가운데 하나의 해쉬 값을 알면 그 노드의 모든 자식 노드에 대해 데이터를 검증할 수 있는 특징이 있다. 이런 특징 때문에 네트워크로 데이터를 전송 받을 경우, 일부 데이터가 손상되었다고 하더라도 어떤 데이터가 손상되었는지를 쉽게 찾아낼 수 있고, 손상된 데이터를 다시 전송받을 수 있는 장점이 있다. 예를 들어 그림 4[23]에서 보는 것과 같이 데이터 “L1” 번이 손상되었다면, 해쉬 “0-0” 과 해쉬 “0” , 그리고 “루트 해쉬” 가 달라지고 다른 값들은 달라지지 않을 것이다. 이러한 방식으로 대량의 데이터가 있을 경우에도 손상된 데이터를 빠르게 찾아낼 수 있다.

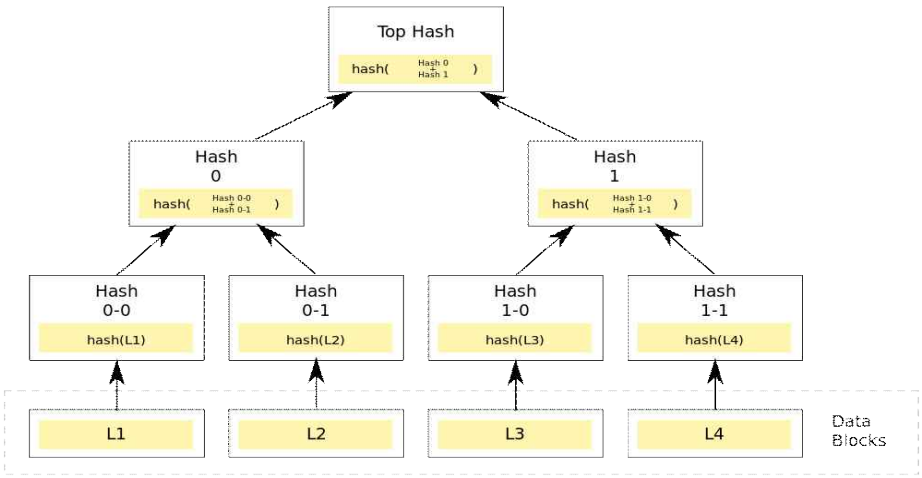


그림 4 해쉬 트리 구조

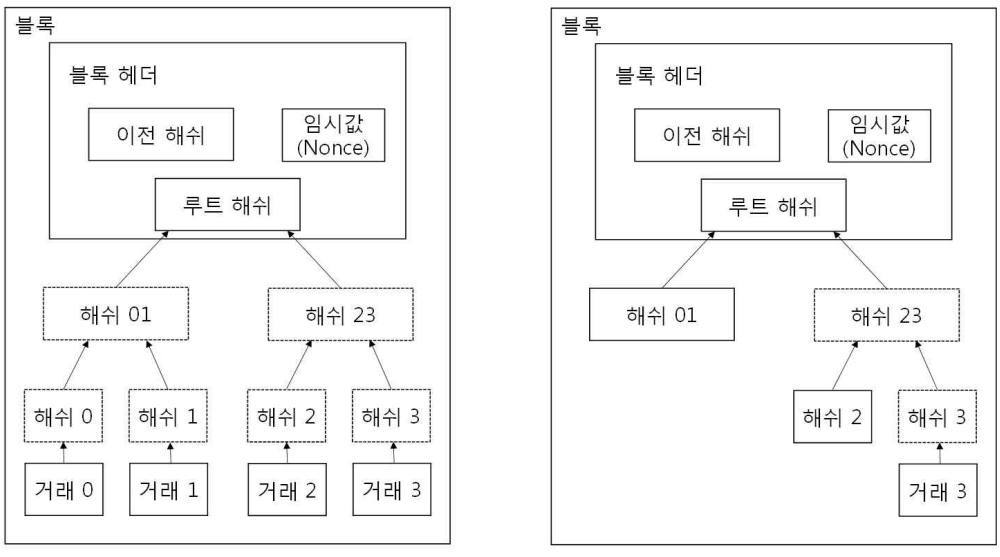
블록체인의 해쉬 트리에 사용되는 암호 해쉬 알고리즘은 SHA256이다. 해쉬 트리에 N개의 데이터들을 해쉬하여 요약하고, N개의 데이

23) <https://ko.wikipedia.org/wiki/%ED%95%B4%EC%8B%9C_%ED%8A%B8%EB%A6%AC> 2016.11.14. 최종검색

터가 담긴 해쉬 트리에서 특정 데이터가 포함되어 있는지를 알아보기 위해서는 최대 $2*\log_2(N)$번의 연산이 필요하기 때문에 매우 효율적인 데이터 구조를 만들어 준다.

해쉬 트리를 사용하여 비트코인 거래 참여자는 블록 헤더(블록당 80바이트)를 다운로드 받고, 수십 기가바이트가 될지도 모르는 거대 규모의 블록체인을 저장하거나 전송할 필요 없이 풀 클라이언트의 전체 거래내역으로부터 작은 크기의 해쉬 경로를 검색함으로써 거래의 포함 여부를 확인할 수 있다. 전체의 블록체인을 보관하지 않는 참여자의 경우, 해쉬 경로를 이용해서 전체 블록을 다운로드하지 않아도 거래를 검증할 수 있다.

해쉬 트리의 루트 해쉬 값만 블록체인의 헤더 부분에 포함되며, 오래된 블록은 트리 구조에서 가지를 정리하므로 더 작아지게 되고, 하위 해쉬는 저장할 필요가 없게 된다.



해쉬 트리 구조로 해쉬된 거래 내역들　　블록에서 거래 내역 0~2를 제거 후

그림 5 해쉬된 거래 내역과 거래내역 제거 후 트리 구조

거래 내역이 없는 볼록 헤더는 대략 80바이트이다. 매 10분마다 블록이 생성되는 비트코인의 경우, 80바이트 * 6 *24 *365 = 4.2 MB가 매년 소요된다. 2008년 기준으로 시중에 판매되고 있는, 2GB 메모리가 장착된 컴퓨터 시스템과, 매년 1.2GB가 증가할 거라 예측한 무어의 법칙(Moore's law)[24]에 의하면, 블록 헤더가 메모리를 점유하고 있어야 하더라도 문제가 되지 않는다.

4.2. 블록체인의 개념

4.2.1. 블록체인의 의의

블록체인(BlockChain)은 분산 데이터베이스의 한 형태이며 지속적으로 성장하는 데이터 기록 리스트로서 분산 노드의 운영자에 의한 임의 조작이 불가능하도록 고안되었다. 앞서 설명했듯이 잘 알려진 블록체인의 응용사례는 암호 화폐의 거래과정을 기록하는 탈중앙화된 전자장부로서 비트코인이 있다. 이 거래 기록은 의무적으로 암호화되고 블록체인 소프트웨어를 실행하는 컴퓨터상에서 운영된다.

블록체인(BlockChain)은 블록(Block)을 잇따라 연결하여 만든 블록의 집합체로써 블록에 일정 시간 동안 확정된 거래내역을 담은 일종의 공공 거래 장부이다. 블록체인은 P2P 네트워크에서 발생하는 모든 거래(Transaction) 정보를 담고 있으며, 이를 모든 참여자가 저장하고 업데이트 한다. 블록체인은 분산데이터 베이스와 유사한 형태로 데이터를 저장하는 구조체 리스트로 네트워크 참여자들이 데이터를 저장 ·

24) 반도체 집적회로의 성능이 18개월마다 2배로 증가한다는 법칙이다. 매년 약 1.59배 증가한다고 예측하고 있다.

검증하여 임의조작이 어렵게 설계되어 있다.

블록체인은 몇 가지 특징을 가지고 있다. 첫 번째로 제3자가 없는 신뢰성을 보장한다. 블록체인 시스템 자체가 그 안에 담긴 기록의 무결성을 증명·보증하므로, 신뢰성을 담보할 중앙 집중적 조직이나 제3자를 필요로 하지 않는다. 두 번째는 경제성이다. 블록체인의 신뢰성을 담보할 중앙 집중적 조직이나 구조가 필요 없어, 시스템 구축 및 유지보수 비용이 적어 비용절감효과를 가진다. 세 번째는 안전성이다. 모든 참여자가 거래 장부를 갖고 있기 때문에 네트워크 일부에 문제가 생겨도 전체 블록체인에 영향이 없으며, 중앙 집중적인 기존 시스템에 비해 안전하다. 네 번째는 거래내역의 투명성이다. 기존 금융거래는 금융회사와 거래 당사자 사이의 비밀과 같이 다른 사람에게는 공개되지 않는 경우가 대부분이나, 블록체인은 모든 거래내역을 기록, 공유함으로써 기존 금융시스템보다 투명하다. 마지막으로 개인 정보를 보호해준다. 휴대폰만 있어도 블록체인을 통해 금융서비스를 이용할 수 있어, 금융회사는 개인정보의 수집·보관·유출의 부담에서 벗어날 수 있다.

4.2.2. 블록체인의 구조

블록체인의 각 블록은 헤더와 바디로 구성된 구조체이다. 헤더에는 이전 블록의 해쉬 값, 해당 블록에 포함된 거래로부터 생성된 해쉬 트리[25] 루트의 해쉬 값, 넌스(Nonce) 등을 포함하고 있다.

25) 해쉬 트리는 여러 블록으로 나뉜 데이터를 전송할 때 데이터가 변조되지 않았음을 보장하는 용도로 사용된다. 특히 P2P 망에서 전송받은 데이터에 오류가 있거나 악의적인 데이터 변조가 있는지를 검증하는 용도로 사용되고 있다.

그림 6 블록체인의 기본구조

이전 블록의 해쉬 값과 해당 블록에 대한 해쉬 값을 포함하여 블록을 생성하므로 블록의 내용을 위 · 변조 할 수 없으며, 거래 정보가 공개되어 있기 때문에 투명하게 관리가 가능하다. 참여자의 과반수를 동시에 해킹한다면 데이터 변조가 가능하지만 현실적으로는 어렵다. 2013년 11월 기준으로 비트코인 총 해쉬량은 전 세계 슈퍼컴퓨터 1위부터 500위까지의 컴퓨팅 파워를 모두 합친 것의 256배 이상으로 추정되었다.[26] 따라서 블록체인의 길이가 길어질수록 블록의 신뢰도는 증가하게 된다.

블록이 어떻게 구성되어 있는지 블록의 전체 구조를 살펴보면 다음과 같다.

필드 [크기]	설명
블록 크기 [4바이트]	- 필드 뒤에 따라 나오는 블록의 크기
블록 헤더 [80바이트]	- 버전(소프트웨어/프로토콜 업그레이드 추적을 위한 버전 번호) [4바이트]

26) 금융보안원, 블록체인 및 비트코인 보안 기술, 2015.11.23.

블록 헤더 [80바이트]	- 이전 블록 해쉬 값 [32바이트] - 해쉬 트리 루트의 해쉬 값 [32바이트] - 타임스탬프 [4바이트] - 블록의 작업 증명 알고리즘에 대한 난이도 목표 [4바이트] - 넌스(작업증명 알고리즘에 사용되는 카운터) [4바이트]
블록 바디 [가변적]	- 거래 카운터 [1~9바이트] - 블록에 기록된 거래 [가변적]

표 1 블록 및 블록헤더의 구조

블록의 헤더 앞에는 블록 크기를 나타내는 4바이트가 온다. 그 다음에 블록 헤더가 위치한다. 블록헤더는 버전, 이전 블록 해쉬 값, 해쉬 트리 루트의 해쉬 값, 타임스탬프, 블록의 작업 증명 알고리즘에 대한 난이도 목표, 넌스로 구성된다. 블록의 검증은 방금 나열한 블록 헤더의 80바이트만 가지고 할 수 있다. 그 다음 블록의 바디가 위치하는데, 거래의 개수를 나타내는 거래 카운터와 블록에 기록 된 거래로 구성된다. 블록에 기록된 거래 내역은 해쉬 트리 구조로 요약하여 효율적으로 관리한다.

4.2.3. 블록체인 생성 방식

최초 블록에서 시작된 블록체인부터 전체의 블록체인을 저장하는 풀 클라이언트를 생성하기 위한 블록체인의 네트워크 동작은 다음과 같은 과정으로 이루어진다. ① 새로운 거래 내역이 모든 참여자에게 알려진다. ② 각 참여자들은 새로운 거래 내역을 블록에 취합한다. ③

각 참여자들은 그 블록에 대한 작업증명을 진행한다. ④ 어떤 참여자가 작업증명을 성공적으로 수행했을 때, 모든 참여자에게 그 블록을 전송한다. ⑤ 참여자들은 그 블록 안에 들어 있는 모든 거래가 유효한 거래인지, 그리고 혹시 이미 다른 블록에서 끝낸 작업이 아닌지를 판단하여 괜찮은 경우에만 승인한다. ⑥ 참여자들은 자신이 승인한 블록의 해쉬를 이전 해쉬로 사용하여 다음 블록을 생성하는 과정을 통해 그 블록이 승인되었다는 의사를 나타낸다. 이를 살펴보면 그림 7[27]과 같다.

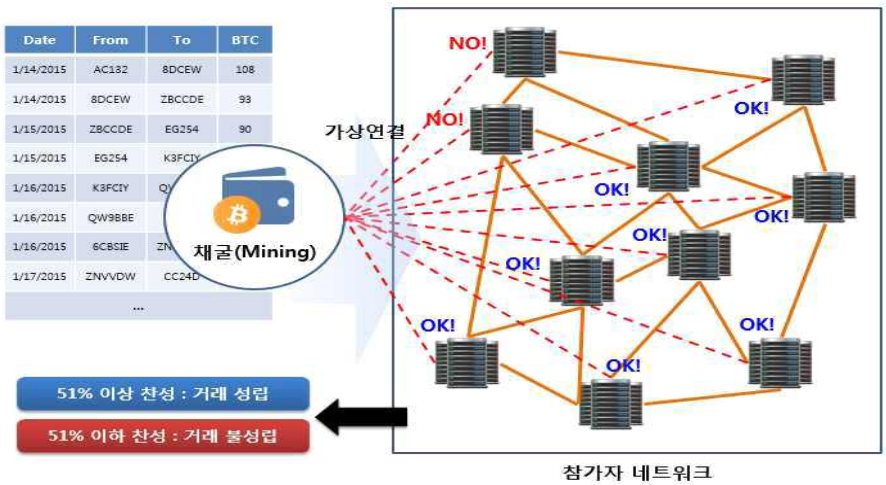
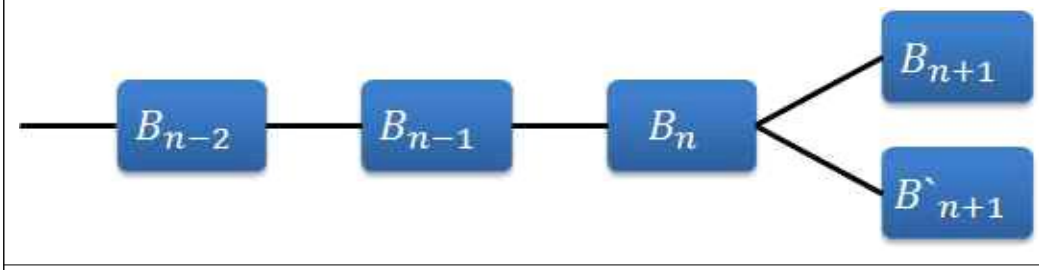


그림 7 분산 합의 과정

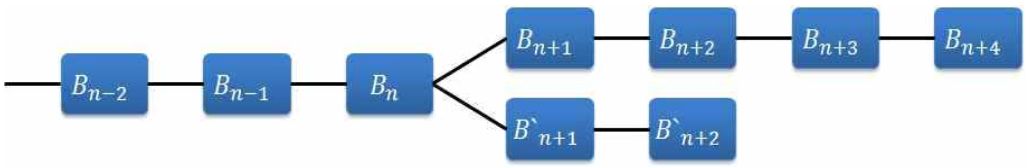
블록을 생성하는 도중에 이중 거래가 일어난 경우, 참여자들은 항상 가장 긴 체인을 옳은 것으로 간주하며 그 체인이 계속 확장하도록 작업을 수행한다. 만약 두 참여자가 서로 다른 버전의 다음 블록을 동시에 알리게 될 경우, 어떤 참여자들은 둘 중 하나를 먼저 전달받게 된다. 이러한 경우 각 참여자들은 자신이 먼저 받은 블록에 대해 작업을 수행하지만, 체인의 다른 갈래도 더 길어질 경우에 대비하여 저장

27) 금융보안원, 블록체인 및 비트코인 보안 기술 (2015)

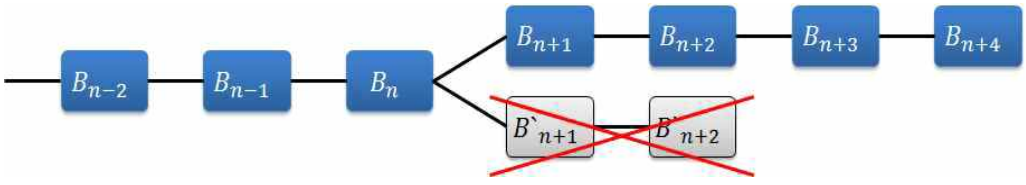
해둔다. 체인의 어느 한쪽 갈래가 더 길게 생성되는 작업증명이 알려지면 체인 갈래의 길이는 더 이상 대등하지 않게 되고, 각 참여자들은 체인이 더 긴 갈래로 작업을 전환한다. 이를 The Longest Chain Wins[28] 매커니즘이라고 부른다. 자세히 살펴보면 표 2[29]와 같다.



① 이용자가 비트코인을 중복으로 사용하여 그 거래 내역이 서로 다른 참여자들에게 전송되면, 두 개의 블록이 생성



② 채굴자들은 두 개의 블록을 가지고 경쟁적으로 다음 블록을 생성



③ 결국 경쟁에서 진 체인은 자연스럽게 소멸

표 2 이중 거래 방지 과정

28) 비트코인은 총 통화량이 정해져 있어서 그 이상은 발행될 수 없다. 이중 거래 발생 시 총 통화량이 초과되고, 초과되는 거래량에 대해서는 The Longest Chain Wins 메커니즘을 이용한다.
29) 금융보안원, 블록체인 및 비트코인 보안 기술 (2015)

새로운 거래 내역 알림이 반드시 모든 참여자에게 전달될 필요는 없으며, 많은 참여자에게 전달될수록 더욱 빠르게 남은 참여자들의 블록에 포함될 것이다. 또한 새로운 거래 내역 알림이 누락되어 해당 블록을 받지 못한 경우가 생겼다고 해도, 다음 블록을 받음으로써 이전의 블록이 누락되었음을 알아차리게 된다. 이러한 경우 이전 블록을 다시 요청하여 받을 수 있으므로 블록이 누락되어 거래내역이 빠지는 경우에 대하여 염려하지 않아도 된다.

풀 클라이언트는 모든 거래내역을 담은 블록들을 가지고 있으며 다른 참여자와 연결을 통해 자기가 가지고 있는 블록 정보를 남에게 줄 수 있다. 즉, 많은 참여자들이 신뢰할 수 있는 공개 장부 전체를 보유함으로써 중앙 통제 기관이 필요 없어진다.

4.2.4. 블록체인 종류

4.2.4.1. 퍼블릭 블록체인

퍼블릭 블록체인은 최초의 블록체인 활용사례로써 인터넷을 통해 모두에게 공개 · 운용 가능한 거래장부이다. 컴퓨팅 파워를 이용한 채굴 (Proof-of -Work) 과정을 통해 거래의 정당성을 인증하며, 개인 또는 중앙기관의 영향을 받지 않는 탈중앙화, 분권화된 시스템이다.

퍼블릭 블록체인은 어느 누구나 블록체인의 데이터를 읽고, 쓰고, 검증할 수 있다. 앞서 언급 했듯이 비트코인이 가장 대표적인 예이다. 비트코인을 사용하는 모든 비트코인 거래 참여자들은 블록체인을 다운로드하여 거래내역을 검증할 수 있다. 참여자들은 어떤 데이터가

입력될지를 투표로 결정한다. 이를 분산 합의 제도라고 한다. 분산 합의 제도는 거래내역을 블록체인에 포함시키기 위해서 거래를 승인하는 방식으로 제3의 신용기관 없이 P2P 분산 네트워크에서 검증한다. 하지만 투표자 수로 데이터의 적법성을 결정하게 되면 비트코인 거래 참여자의 수를 무작위로 늘리는 스팸 공격이 일어날 수 있기 때문에 참여자의 수가 아니라 투입한 컴퓨팅 파워에 비례해서 투표권을 부여한다. 참여자들은 이렇게 얻은 투표권을 통해 각 블록의 데이터 무결성을 검증하고 작업증명(Proof-of-Work, PoW)에 참여한다. 일반적으로 퍼블릭 블록체인의 보안은 암호와 각 블록에서 제공하는 금전적 이익에 의해 유지된다. 따라서 언제든 더 큰 경제적 동기(economic incentive)가 존재한다면 시스템 자체가 무너질 수 있는 결함이 존재한다. 또한 기록에 문제가 생긴 경우에도 수정이 어려우며, 비밀 데이터를 포함한 모든 데이터가 무차별적으로 공개되어 비밀이 유지되기 어렵다는 점과 참여자들의 신원이 공개되지 않아 불법적인 익명거래 등에 사용될 수 있다는 단점이 있다. 이 외에도 많은 한계들과 비트코인의 고유의 특징들이 퍼블릭 블록체인을 채택할 수 없도록 만들고 있다. 위와 같은 문제점에 봉착한 경우, 이러한 문제의 해결에 나설 중앙기관이 없기 때문에 시스템을 유지하기 위한 복잡성과 불완전성이 내재되어 있다. 또한 네트워크 확장이 어렵고 거래 속도가 느리다는 등의 이유도 한계로 작용한다. 이러한 점들을 보완하기 위해서 새로운 방식의 블록체인이 대안으로 논의되고 있다.[30]

퍼블릭 블록체인을 실제로 활용하고 있는 기업들을 보면 다음과 같다. Ethereum은 스마트 계약을 실행하고 개발자가 분산 응용 프로그

30) <http://www.seunghwanhan.com/2016/10/public-blockchain-and-private-blockchain.html 와 https://brunch.co.kr/@jeffpaik/5> 2016.11.14. 최종검색

램을 게시 할 수 있게 해주는 분산 플랫폼 및 프로그래밍 언어 공급자이다. 레코드 관리 업체인 Factom은 기업 및 정부를 위한 비즈니스 프로세스를 기록하고 관리한다. Sidechain 기술 제공 업체 인 Blockstream은 퍼블릭 블록체인 기술을 사용하여 회계업무를 할 수 있도록 연구하기 시작했다.

4.2.4.2. 프라이빗 블록체인

프라이빗 블록체인은 완전히 개인화된 블록체인으로서 중앙 기관이 모든 권한을 가지며 네트워크에 참여하기 위해서는 그 중앙기관의 허락이 필요하다. 즉, 1개의 주체가 내부 전산망을 블록체인으로 관리하는 것이다. 이것은 중앙 권한기관이 필요에 따라 규칙을 변경하거나 트랜잭션을 되돌릴 권한을 갖는 기존 인프라 유사하다. 기업이나 공공기관에서 중앙시스템을 구축하여 비용을 줄이면서 동시에 효율성을 높이기 위해 사용할 수 있다.

프라이빗 블록체인은 읽기, 쓰기, 합의 과정에 참여할 수 있는 참여자가 미리 지정되어 있으며, 필요에 따라 특정 주체를 새로 추가하거나 제거할 수 있다. 또한 설계 목적에 따라 자신에게 맞는 버전으로 프라이빗 블록체인을 설계할 수 있다. 다시 말하면 모두가 자료를 조회할 수는 있으나 자료의 기록은 특정 주체만 가능하게 할 수도 있고, 또는 조회와 기록을 모두 특정 주체만이 가능하게 할 수 있는 등 다양한 방식으로 권한 수정이 가능하다. 예를 들어 금융업무의 경우, 읽기 권한은 거래 당사자와 거래를 감독할 의무가 있는 금융감독기구 및 중앙은행에게 주어지고, 쓰기 권한과 합의 알고리즘을 통한 검증 권한은 모든 거래 참여자에게 주어질 수 있고, 수사기관에서 응용하는

경우를 생각한다면 중앙에서만 쓰기 권한을 갖고, 네트워크 참여자에게는 읽기 권한만 부여하여 중앙에서 블록체인을 생성하여 관리하고, 참여자에게는 열람 권리만을 제공하는 방식으로 디지털 데이터를 관리할 수 있다. 이렇게 프라이빗 블록체인은 접근권한 설정을 각각의 사용 환경에 맞게 수정할 수 있다는 장점이 있어, 목적에 따라 맞춤형으로 설계가 가능하다.

현재까지 제작되고 있는 프라이빗 블록체인은 대부분 PoW를 통한 “해쉬파워 경쟁모델”은 아니고, PoS 또는 FBA(Federated Byzantine agreement), BTF, Tendermint, PBFT protocol, PoTE, HoneyBadgerBFT 등과 같이 해쉬경쟁이 없는 알고리즘을 사용하고 있다. 다시 설명하면, 퍼블릭 블록체인에서는 악의적인 목적으로 동시에 두 곳 이상의 계좌로 송금하는 행위를 방지하기 위해서 총 통화량[31], The Longest Chain Wins 메커니즘을 이용한다. 하지만 프라이빗 블록체인에서는 해쉬경쟁이 없는 알고리즘을 사용하여도 중앙에서 악의적인 목적의 이중 거래를 차단하는 등의 관리를 할 수 있기 때문에 퍼블릭 블록체인과 같이 총 통화량이나 The Longest Chain Wins 메커니즘을 이용할 필요가 없다.

프라이빗 블록체인 솔루션은 퍼블릭 블록체인처럼 해쉬경쟁에 의존하지 않아도 충분히 보안성을 제공한다. 서버를 분산시키는 것 자체로 보안을 높일 수 있으며, 처리비용과 시간의 절감을 위한 솔루션으로 사용되기 때문이다. 중개기관을 거칠 필요 없이, 서로 다른 참여자가 자신의 데이터를 온전히 신뢰할 수 있게 된다면 데이터 오차수

31) 비트코인은 총 통화량이 정해져 있어서 그 이상은 발행될 수 없다. 이중 거래가 발생하는 경우 총 통화량이 초과되고, 초과되는 거래량에 대해서는 The Longest Chain Wins 메커니즘을 이용하여 이중 거래를 방지한다.

정, 불일치 내역 조정, 커뮤니케이션을 위한 메시징 시간 절감 등 혁신적인 변화를 기대할 수 있다. 특히 금융기관의 경우, 이러한 데이터 처리 속도증가는 곧 지급 및 결제 속도의 증가로 이어지며, 관련 비용은 물론 거래상대방 리스크와 유동성 리스크를 획기적으로 줄일 수 있게 돕는다.[32] 다음에 기술할 수사기관의 증거관리에서도 마찬가지이다. 여러 이용자가 동시에 또는 일정 시간대에 작업을 할 가능성이 있는 데이터 등록 · 폐기의 경우, 데이터처리의 속도증가는 효율적인 관리로 이어진다.

프라이빗 블록체인을 실제로 활용하고 있는 기업들을 보면 다음과 같다. Eris Industries는 블록체인 사용하여 공유 소프트웨어 데이터베이스를 제공한다. Blockstack은 프라이빗 블록체인을 이용하여 지불이나 정산을 비롯한 금융기관의 업무를 제공한다. Multichain은 금융 거래를 위한 오픈 소스 분산 데이터베이스를 제공한다. 블록체인 API 공급자인 Chain Inc.는 나스닥 OMX 그룹과 파트너 관계를 맺어 나스닥 프라이빗 마켓에 블록체인 기술을 적용하여, 비상장 주식 거래를 할 수 있는 플랫폼을 제공하고 블록체인 인프라를 공유하는 기업들과 파트너십을 발표하는 등 활발하게 연구를 진행하고 있다.

4.2.4.3. 컨소시엄 블록체인

컨소시엄 블록체인은 미리 선정된 네트워크 참여자에 의해서 컨트롤 되는 반 중앙형 블록체인이다. 이것은 조직이나 기업들이 서로 협력하여 다른 모델을 개발하는데 사용할 수 있다. 미리 선정된 N개의 주체들을 참여시키고 각 기관 사이의 동의가 일어나야 거래가 생성된

32) <http://www.seunghwanhan.com/2016/10/public-blockchain-and-private-blockchain.html>, <https://brunch.co.kr/@jeffpaik/5> 2016.11.14. 최종검색

다. 또한 N개의 주체들 간의 합의된 규칙을 통해 공증에 참여하며, 네트워크 확장이 용이하고 거래 속도가 빠르다는 장점이 있다. 따라서 블록체인의 기록을 열람할 수 있는 권한을 퍼블릭 블록체인처럼 대중에게 부여할 수도 있지만 네트워크 참여자에게만 제공하거나 API (Application Programming Interface)[33]를 통해 특정 인원에게만 공개할 수도 있다. 즉, 컨소시엄 블록체인은 미리 선정된 특정 거래 증명자들에 의해서 통제되는 블록체인으로, 한정된 탈중앙화적 요소와 분산장부의 특징을 이용한 부분적 분산형태의 블록체인이다.

4.2.5. 블록체인의 활용분야

블록체인은 현재 금융권에서 가장 활발하게 활용되고 있으며, 그 외에도 일반적인 분야에서 활용되고 있다. 블록체인은 비트코인 이외에도 전자화폐, 대출, 해외송금, 주식거래, 의료서비스, 소유권 증명, 에스크로, 데이터 및 메시지 보안 등 다양한 분야에서 활용되고 있다. 금융권의 블록체인 활용 사례를 간단하게 정리하면 표 3[34]과 같이 주로 통화 교환 및 송금, 주식거래, 메시지 보호나 데이터 저장 등에 응용하여 사용하고 있다.

통화 교환 및 송금	P2P 송금	공동소유	데이터 저장	주식거래 플랫폼	게임
					

표 3 금융권의 블록체인 주요 활용 분야

33) 응용 프로그램에서 사용할 수 있도록, 운영 체제나 프로그래밍 언어가 제공하는 기능을 제어할 수 있게 만든 인터페이스를 뜻한다.

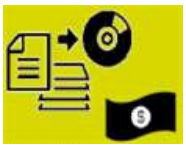
34) <https://letstalkpayments.com/an-overview-of-blockchain-technology/> 재구성 2016.11.14. 최종검색

해외에서도 금융권을 중심으로 블록체인에 대한 연구가 활발하게 진행되고 있다. 미국, 영국, 독일, 네덜란드 등 세계 각국에서 전자화폐 지급결제 시스템, P2P 대출 및 송금, 자산등기, 자금세탁방지, 주식매매시스템 서비스 개선 등 다양한 사례가 연구되고 있다. 최근에는 국내에서도 블록체인에 대한 관심이 많아지면서, 금융권을 중심으로 다양한 연구가 진행 중이다. 현재 신한은행, 국민은행, 하나은행, 농협에서 외환 송금서비스나, 개인인증 서비스, 핀테크 등에 블록체인을 적용하기 위하여 관련 기술 업체와 개발 중이다.

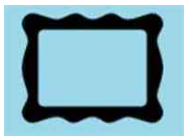
블록체인은 금융기관에만 국한되지 않고, 다양한 분야에서 활용되고 있다. 온두라스에서는 국가 토지 대장을 블록체인을 통해 기록하여 해킹 및 조작을 원천적으로 방지하고 있다. 비트 메시지는 사용자가 만든 P2P 네트워크에서 메시지를 암호화하여 송수신하며 사용자의 주소를 추적할 수 없다. 최근에는 실제 자산을 블록체인에 연결하여 디지털 방식으로 거래하는 방법이 등장하면서, 블록체인을 통해 인증을 받고 부동산 소유권을 설정하거나, 금 · 은 · 다이아몬드의 거래를 검증하는 등 다양한 시도가 이루어지고 있다. 아래의 표 4[35]는 블록체인을 활용한 주요 서비스와 기업들을 정리한 것이다.

구분	주요 서비스	기업
	• 응용 프로그램 개발 모듈의 소유권 증명	Assembly

35) <https://letstalkpayments.com/an-overview-of-blockchain-technology/> 재구성 2016.11.14. 최종검색

구분	주요 서비스	기업
	• 디지털 콘텐츠 저장 및 전달에 대한 소유권 증명	Blocktech (Alexandria), Bisantyum, Blockparti, The Rudimental, BlockCDN
	• Ride Sharing을 위한 포인트 기반의 가치 전송	La'Zooz
	• 문서/계약의 디지털화 및 전송의 소유권 증명	Colu(Colored Coins)
	• 블록체인 상의 컴퓨터 네트워크를 이용한 분산형 스토리지	Company: Storj
	• 클라우드와 홈 네트워크 연결 및 (홈 오토메이션을 위한) 전기 장치를 연결하는 플랫폼	Filament, Chimera IoT
	• 기업 합병 디지털화, 주식/소유권/지배 구조 이전 등에 대한 회사 설립 디지털화	Otonomos
	• 디지털 자산 구매/판매를 위한 시장 활동의 증명 및 소유권 증명	MyPowers

구분	주요 서비스	기업
	• 소비자의 개인 정보를 보호하는 디지털 신분증 제공	Sho Card, Uniquid
	• 게임 산업/대출 서비스/전자상거래를 위한 에스크로/보관 서비스	PlayCoin, BitnPaly New System Technologies, Fundrs.org
	• 전자상거래/제조업에서 주문 처리 수행을 위한 스마트 계약 IT 포털	UbiMS
	• 환자의 진료 기록을 분산하여 관리	BitHealth (Healthcare IT)
	• 자산의 디지털화 : 위조 방지 조치 개선	• Consumer electronics, Automotive : The Real McCoy, Chain Linl, EverPass • Degree Verification : Degree Of Trust

구분	주요 서비스	기업
	• 직원들간의 동료간 평가에 대한 신뢰 가능한 보증을 통해 평가의 신뢰성 활성화	TRST.im
	• 디지털 콘텐츠에 대한 소유권 증명	• Arts, Picture and images : Blockai, Bitproof, ascribe, Artplus, Chainy.Link
	• 소비자의 개인정보 보호를 위한 디지털 신분증 제공	• Internet, Car locks : Onename • Elections Voting : Follow My Vote • Customer identification : Trustatom
	• 주식시장, 경영 등을 위한 분산 예측 플랫폼	Augur

구분	주요 서비스	기업
	• 평가의 진정성 보장(사용자가 참여하고 평판을 공유하여 의견을 수집하는 방식, 신뢰할 수 있는 보증을 통한 방식)	The World Table, Asimov
	• 디지털 보안 거래 : 소유권 및 전송	Symbiont, Mirror, Spritzle, Secure Assets, BitShares, Coins-e, equityBits, DXMarkets, MUNA

표 4 비금융권의 블록체인 주요 활용 분야

5. 블록체인을 이용한 디지털 데이터의 관리 방식 제안

5.1. 들어가는 글

블록체인을 이용하여 디지털 데이터를 어떻게 관리할지 검토해보고자 한다. 검찰의 D-NET에서 생성되는 로그를 모아 블록체인의 거래내역 같이 기록한다면 안전한 관리 방법이 될 것이다. 검찰의 “압수대상으로서의 디지털증거 관리 매뉴얼” 에 따르면, NDFC에서 수사와 관련된 디지털 데이터를 보관하거나 폐기하는 경우 확인서를 이용하여 압수한 전자정보에 대한 처분 내용을 확인하고 있다.

위 매뉴얼에 따르면 압수한 전자정보는 예외적으로 범죄사실과 관련성이 인정되지 않는 경우를 제외하고, 일반적인 경우에는 D-NET에 보관한다. 그리고 압수한 전자정보의 처분은 수사단계에서 압수의 필요성이 없다고 인정되거나 판결에서 몰수선고를 하지 않았을 경우에 일반적으로 이루어지게 된다. 유체물인 압수물의 경우 제출인에게 환부하는 것이 원칙이나, 무체물인 디지털 데이터는 복제된 전자정보로써 재산적인 가치가 없고, 수사 또는 재판 목적 소멸시 이를 폐기할 것을 피압수자에게 사전 고지하기 때문에 보관의 목적이 없어진 디지털 데이터는 폐기 처분한다.

위 매뉴얼에서는 압수한 디지털 데이터를 D-NET에 등록하거나 삭제하는 등의 관리 절차를 정하고, 관련된 행위에 대한 확인서를 출력하여 수사기록에 첨부토록 하여 압수한 디지털 데이터의 보관이나 폐기를 확인하고 있다. 하지만 확인서에 기재된 보관이나 폐기에 대한 실질적인 확인은 과학적인 검증이 필요해 보인다. 서버에서 해당 디

지털 데이터에 대한 로그를 생성하고 이를 자동으로 해쉬하고 저장하여 해쉬 값을 확인하는 방법으로 로그의 무결성을 보장한다면 데이터의 보관 · 삭제 등의 행위 이력을 객관적으로 검증할 수 있을 것이다. 또한 블록체인 관리 방식과 CCTV나 기타 보조적인 수단을 활용한다면, 피압수자가 참관하지 않음에 동의한 경우에는 압수한 디지털 데이터를 문서로 출력하거나 파일로 복제하는 등의 행위를 수사상 필요한 범위 내에서 하였고, 이와 관련하여 적절한 감시 조치를 취하였음을 증명할 수 있을 것이다. 이러한 방안은 디지털 증거 관리의 투명성을 제고할 뿐만 아니라, 디지털 증거 관리 시스템에도 큰 변화를 가져올 수 있을 것이다.

그밖에도 블록체인은 기업의 기밀 유출 방지를 위해 사용되는 문서중앙관리서버에서도 활용이 가능하다. 기존의 문서중앙관리서버는 사용자가 문서에 열람 · 편집 · 인쇄 · 복제 등의 행위이력을 기록하고, 문서에 접근 권한을 설정하여 통제한다. 기록된 행위이력들을 블록체인 방식으로 관리한다면 행위이력의 수정이 어려워져 기업의 문서보안 강화에 유용하다. 이는 기업의 기밀을 유출한 자나 전산 담당자가 해당 행위이력을 수정할 수 없기 때문이다.

5.2. 디지털 증거 관리에 적합한 블록체인 기술의 선택

풀 클라이언트와 퍼블릭 블록체인 방식을 사용하는 블록체인은 디지털 증거를 관리하는 용도로는 알맞지 않다. 풀 클라이언트 방식을 활용하면 전체 블록체인 복사본을 모든 참여자가 가지고 있어야 한다. 전체 블록체인 복사본의 크기는 압수한 디지털 데이터를 등록 · 삭제하는 등의 로그가 생성될 때 마다 점점 더 커질 것이다. 블록체인

의 크기가 커질수록 네트워크의 보안성을 높여주고 외부공격으로부터 안전해질 수 있으나, 블록을 송수신함에 많은 시간과 저장 공간을 필요로 한다. 모든 참여자가 커다란 저장 공간을 가지고 있어야 하며 느린 속도를 감수해야 한다는 점에서 디지털 증거를 관리하는데 맞지 않을 수 있다. 따라서 풀 클라이언트보다는 중요한 부분만을 저장하는 방식이 효율적이다.

또한 퍼블릭 블록체인을 사용한다면 모든 사람이 D-NET의 로그 기록을 열람할 수 있게 된다. 이는 보안이 중요시되는 수사 환경에서 활용하기에는 무리가 있으며, 10분에 한번 거래가 생성되는 비트코인과 비교해볼 때 속도나 효율성 측면에서도 적용하기에는 어려움이 있다. 이러한 단점을 보완한 것이 프라이빗 블록체인이다. 프라이빗 블록체인은 사용자가 원하는 목적에 맞추어 블록체인을 설계할 수 있다.

블록체인을 어떤 방식으로 설계할 지 검토하기 전에 먼저 퍼블릭 블록체인과 프라이빗 블록체인의 장단점을 비교해보겠다. 퍼블릭 블록체인은 누구나 익명으로 참여가 가능하기 때문에 무법적 요소가 강하고, 네트워크에 참여한 컴퓨팅 파워를 51% 해킹하는 공격의 위험성이 존재한다. 물론 참여자의 수로 네트워크를 장악하는 Sybil attack (DDos 공격)을 막기 위하여 채굴 과정이 필요하며, 참여자의 수가 아닌 컴퓨팅 파워에 증명권리를 부여하면서 소수의 네트워크 장악을 막는 채굴은 보안적인 면에서는 훌륭하다고 할 수 있다. 그러나 네트워크를 유지하는데 많은 비용을 소모하며, 네트워크 확장이 어렵고, 채굴 과정으로 인하여 거래 속도가 느리다. 또한 관리하는 규칙을 바꾸는 것이 굉장히 어렵다는 단점이 있다.

반면에 프라이빗 블록체인은 거래 참여자가 관리자에게 인증을 받아 참여하는 형태로 관리자가 거래 참여자를 이미 알고 있는 상태이기 때문에 퍼블릭 블록체인과는 다르게 51% 공격을 피할 수 있다. 프라이빗 블록체인은 분산 저장 방식이 아니라 중앙에서 블록체인을 저장하고 관리하는 방식이기 때문에 사용하는 기관의 성격에 맞게 규칙을 바꿀 수 있고, 네트워크 유지비용이 퍼블릭 블록체인에 비해 적게 든다. 그리고 네트워크 확장이 쉽고 거래 속도가 빠르다는 장점과 프라이빗 블록체인과 같이 로그 기록을 증명하는 유일한 개체가 하나의 기관이라면 Sybil attack 자체가 무의미하다는 장점도 있다.

검토한 내용을 종합하여 보면 Headers-only Clients와 프라이빗 블록체인을 활용하는 방식이 적절해 보인다. Headers-only Clients를 응용하여 몇 개의 서버에서는 전체의 내용을 저장하고, 또 다른 서버에서 블록의 헤더 정보를 블록체인으로 저장하고 이를 백업용 자기 테이프에 영구 보존하는 방법으로 관리한다. 이러한 저장방식에 프라이빗 블록체인 기술을 활용하여 저비용의 빠르고 효율적인 디지털 증거 관리 시스템을 구축하는 방식을 검토해볼 수 있겠다. 프라이빗 블록체인으로 시스템을 구축한다면 실시간으로 블록체인을 생성하여, 여러 개의 서버에 분산 저장할 수 있으며, 수사기관의 디지털 증거 관리 시스템은 보안상 로그를 외부에 공개하지 않으면서도 블록체인에 담긴 해쉬 값으로 명확한 법적 이해관계를 위하여 내부의 로그들을 검증할 수 있다. 블록체인을 공개하지 않고 중앙에서 관리한다는 이유로 데이터 조작에 대해 문제를 제기할 수도 있는데, 이는 로그에 대한 해쉬 값을 제3의 기관에 보내어 보관하거나 인터넷 웹 사이트에 공개하는 방식으로 데이터 조작에 대한 문제를 해결할 수 있다. 이하에서는 구체적인 블록체인의 구성 등에 대해서 살펴보고자 한다.

5.3. 블록체인의 구조 및 시스템 구성 방안

블록체인의 구조를 살펴보기에 앞서 D-NET에서 생성되는 어떤 로그들을 관리할지 살펴보고자 한다. 검찰의 D-NET에서 사용자가 각 사건의 디지털 데이터에 행한 로그를 각각 Object ID, Time Stamp, 해당 데이터의 등록 시간, 어떠한 작업을 한 경우 그 행위를 한 시간, 행위 유형, 행위 직원의 ID, 행위 직원의 소속부서, 수사담당자 ID, 수사 담당자의 부서 등의 정보를 분류하여 아래와 같이 문서 파일 형식으로 저장한다.

Object ID	Time Stamp	등록 시간	사건 번호	지원 번호	증거 번호	파일 이름	행위 유형	행위 직원 ID	행위 직원 부서	Hash
XXX	2016-11-13 11:13	2016-11-13 11:13	2016 형제 1234	2016 지원 1234	2016 증거 1234_001	회계 자료.xlsx	등록	홍길동	00 지검 00 부	…
YYY	2016-11-13 11:33	2016-11-13 11:13	2016 형제 1234	2016 지원 1234	2016 증거 1234_002	인사 자료.hwp	열람	이순신	00 지검 00 부	…

표 5 D-NET의 로그를 기록해 놓은 데이터베이스 테이블

로그가 만들어질 때 저장된 문서 파일을 해쉬하고, 문서 파일에 담긴

내용들과 그 해쉬 값을 함께 “행위 이력 관리 서버1” 의 데이터베이스에 기록하고 저장한다. “행위 이력 관리 서버1” 에 저장한 로그들을 DB Trigger[36] 기능을 이용하여 “행위 이력 관리 서버2” 에 저장한다. 그 다음 이를 검증하기 위한 블록의 헤더 정보를 여러 개의 “블록체인 관리 서버” 에 저장한다. “블록체인 관리 서버” 에 저장된 블록체인은 주기적으로 자기 테이프에 백업하여 보관한다. 또한 문제 발생 시 관련된 로그를 쉽고 신속하게 검색하기 위해 “행위 이력 관리 서버2” 의 데이터베이스에 인덱스[37]를 생성하여 관리한다. 각각의 서버를 관리하는 담당자를 서로 다르게 하고, 서버간의 접근을 제한하여 감시한다면 신뢰할 수 있는 디지털 증거 관리 시스템이 될 것이다. 다만, 중앙 관리 방식이기 때문에 로그를 조작하였다는 의심에서 자유롭지 못할 수 있다. 이런 문제의 해결을 위해 로그에 대한 해쉬 값이나 “블록체인 관리 서버” 에 저장된 블록체인을 법원이나 신뢰할 수 있는 제3의 기관에 보관하게 하거나, 모두가 신뢰할 수 있는 인터넷 사이트에 공개하는 방식으로 로그에 대한 수정이 없었음을 보장한다면 블록체인을 이용한 디지털 증거 관리시스템의 신뢰성을 더욱 높일 수 있을 것이다.

---

36) 테이블에 대한 이벤트를 자동으로 실행해주는 DML(데이터조작언어) 데이터 상태의 관리를 자동화하는 기능이다.

37) 나무(Tree)처럼 가지에 해당하는 브랜치 블록(Branch Block)과 잎에 해당하는 리프 블록(Leaf Block)이 있다. 가장 상위에 존재하는 루트(Root)를 기준으로 브랜치 블록들의 깊이(Depth)가 동일하다. 모든 Leaf 블록이 같은 높이에 위치하도록 유지한다. 데이터를 가진 블록에 탐색 시간을 동일(일정)하게 유지한다. 그러나 노드 블록에 접근 시간(Access time)이 동일(일정)한 것은 아니다. 그래서 균형(Balaced)이 잡혀있다. leaf block은 정렬(sorting)되어 있으며, 키 값의 내림차순은 물론 오름차순의 키 값으로 인덱스를 검색하는데 편리하도록 양방향(doubling)으로 연결(link)되어 있다. insert 발생 시 leaf block의 오른쪽으로 성장(즉, 오른쪽으로 insert 됨)하며 insert 후에 재정렬 작업 수행한다.

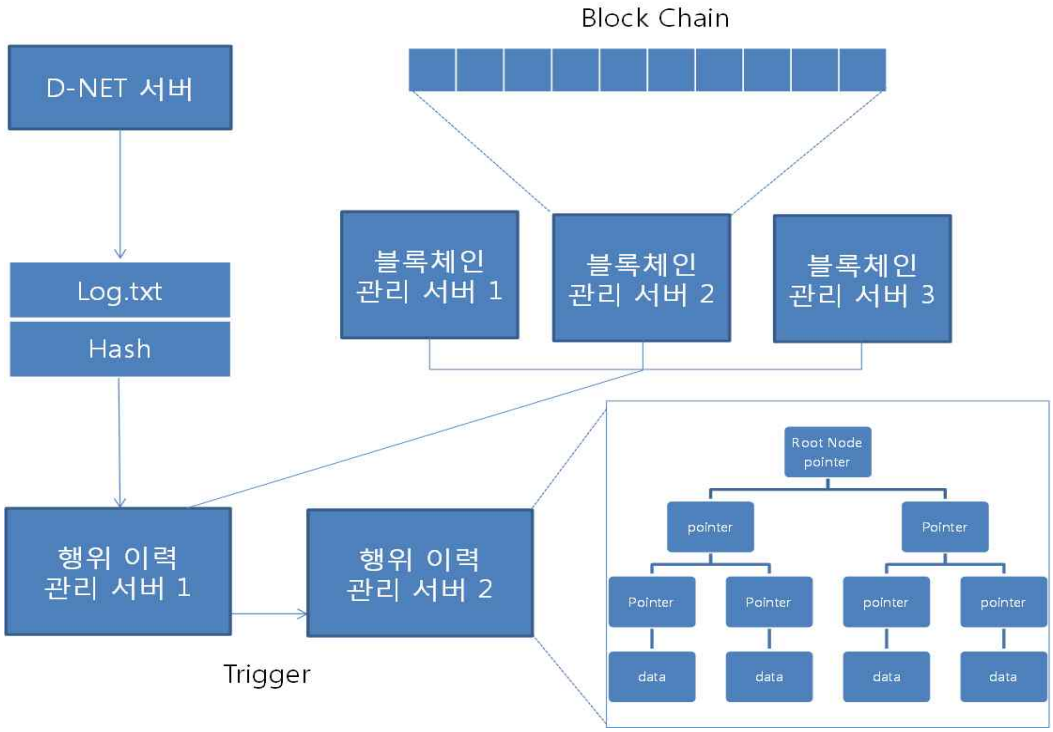


그림 8 블록체인을 기반으로 한 디지털증거관리시스템 구성

“블록체인 관리 서버”에 저장된 블록의 기본적인 구조를 살펴보면 표 6과 같다. ① 버전, ② 이전 블록의 해쉬 값, ③ 현재 로그의 문서 파일 해쉬 값, ④ 타임스탬프 이렇게 기본적인 4가지 요소로 구성한다. 다른 기타 정보들을 추가 구성할 수 있으나 구체적인 구조는 추후 실제 시스템을 구축하는 단계에서 논의해야할 것이다.

크기	필드	설명
4바이트	버전	소프트웨어/프로토콜 업그레이드 추적을 위한 버전 번호
32바이트	이전 블록 해쉬	이전 로그(행위 이력)을 담은 문서 파일의 해쉬 값

크기	필드	설명
32바이트	현재 블록 해쉬	현재 로그(행위 이력)을 담은 문서 파일의 해쉬 값
4바이트	타임스탬프	블록의 생성 시간

표 6 블록 구조

5.4. 보관 및 폐기 검증

블록체인을 이용하여 어떻게 디지털 데이터의 보관·폐기에 대한 행위 이력을 확인할지 검토해보고자 한다. D-NET에서 생성되는 로그를 문서 파일로 만들고, 이러한 문서 파일을 해쉬하여 해쉬 값과 해당 로그를 함께 저장한다. 그림 9은 Object ID, Time Stamp 등의 항목과 그 항목을 담은 문서 파일의 해쉬 값을 저장한 데이터베이스의 테이블이다. 문서 파일에 저장된 행위 이력에 대한 Hash 1을 생성하고, 그 값을 블록 1에 저장한다. 그 다음 생성된 로그를 해쉬하여 Hash 2를 생성하고, 블록 1의 Hash 1과 새롭게 생성한 Hash 2를 블록 2에 저장한다. 같은 방법으로 블록 3에 Hash 2와 Hash 3을 저장하여 해쉬 값으로 블록을 연결한다. 로그가 생성됨에 따라 위의 방법이 반복되면서 블록체인이 생성되는 것이다.

이와 같이 이전 블록의 해쉬 값을 체인으로 연결하여 저장·보관함으로써 하나의 행위 이력에 대한 무결성이 보장되는 것은 물론이고, 블록체인이 점점 축적되어 중간에 얽혀 저장된 행위 이력에 대한 변조 가능성은 제로에 가까워진다. 이러한 이유로 데이터베이스에 저장

되어 있는 행위 이력에 대한 수정은 시간이 지날수록 불가능에 가까워지며, 해쉬 값이 같음을 확인함으로써 수정되지 않았음을 검증할 수 있다.

그림 9 데이터베이스에 저장된 테이블의 내용과 블록체인 구조

검찰에서 시행한 “압수대상으로서의 디지털 증거 관리 매뉴얼”의 보관 · 폐기 확인서에 본 논문에서 제안하는 관리 방식을 적용시켜 보면, 해당 디지털 증거의 행위 이력에 대한 해쉬 값을 기재하고, 추후에 이를 비교하는 방법으로 해당 행위 이력이 수정되지 않았음을 확인할 수 있다. “디지털 증거 보관 확인서”를 예로 들면, 확인서에 디지털 증

거 등록시 남긴 행위 이력의 해쉬 값과 디지털 증거명, 보관 증거번호 등을 기재하고, 해당 사건의 수사검사 서명을 받아서 사건 기록에 편철하여 보관한다. 이러한 행위에 대해 수정이 없음을 검증하기 위해서는 기록에 편철된 확인서와 블록체인 관리 서버에 저장된 해쉬 값을 비교하여 확인할 수 있다. “디지털 증거 보관 확인서”는 아래 그림 10과 같다.

[붙임 5]

National Digital Forensic Center

디지털증거 보관 확인서

피의자 *홍길동*에 대한 *서울중앙지방검찰청 2016형제12345호(2016요청00012호, 2016요청00456호, 2016요청01222호)* 사건에 관하여 대검찰청 국가디지털포렌식센터(NDFC)에 보관되어 있는 디지털증거는 다음과 같습니다.

순번	디지털증거명	용량	등록일시	담당포렌식수사관	보관증거번호	보관 Hash 값
1	*홍길동의 PC1 논리이미지*	*150MB*	*2016. 3. 10. 15:00*	*검찰주사 김태백*	*2016증거00012_0001_1_0001*	*a59622d5b9f521135a5f070ce53833c0*
2	*홍길동의 USB 논리이미지*	*450MB*	*2016. 3. 16. 13:00*	*검찰주사 김백두*	*2016증거00456_0001_2_0001*	*b18322d5b9f5df3d6c52f7c8e53d2c40*
3	*김산악의 CCTV 증거파일*	*200MB*	*2016. 4. 20. 13:00*	*검찰주사 김한라*	*2016증거01222_0001_1_0001*	*c533d234fb26221c8b4fd40c2de83c20*

위와 같이 디지털증거가 보관되어 있음을 확인합니다.

20 . . .

대검찰청 디지털수사과 관리책임자 *이 무 등* *(전자서명)*

검찰청 지청 검사 ○ ○ ○

그림 10 보관 해쉬 값을 활용한 디지털 증거 보관 확인서

디지털 증거를 폐기하는 경우에도 “디지털 증거 폐기 확인서”에 폐기 행위 이력의 해쉬 값을 기재하여 이를 출력 후 사건 기록에 편철한다. 위에서 설명한 보관 확인서와 같은 방법으로 해쉬 값을 비교하여 검증한다면 확인서로서의 역할을 충분히 할 수 있을 것이다.

[붙임 4] 디지털증거 폐기 확인서

National Digital Forensic Center

디지털증거 폐기 확인서

피의자 *홍길동*에 대한 *2016형제12345호(2016요청01456호)* 사건에 관하여 *2016. 5. 20. 15:20 검사 이몽룡의 폐기 지휘*에 따라 대검찰청 국가디지털포렌식센터(NDFC)에서 폐기한 디지털증거는 다음과 같습니다.

순번	디지털증거명	보관 증거번호	용량	등록일시	폐기일시	폐기 Hash 값	폐기방법
1	*김우주의 삼성 스마트폰 몰리 이미지*	*2016증거 01456_0001 _2_0001*	*16GB*	*2016. 4. 16. 15:00*	*2016. 5. 27. 17:00*	*a59622d5b9f5 21135a5f070c n53833c0*	*D-NET에서 삭제*

위와 같이 디지털증거를 폐기했음을 확인합니다.

20 . . .

대검찰청 디지털수사과 관리책임자 ***이 무 등*** *(전자서명)*

그림 11 폐기 해쉬 값을 활용한 디지털 증거 폐기 확인서

6. 결론

지금까지 디지털 데이터의 개념 그리고 디지털 증거의 특징 및 요건에 대해서 정리한 뒤, 디지털 데이터 관리방법의 한계와 최근 검찰에서 디지털 증거에 대해 논의되고 있는 사항들을 다루어 보았다. 그 다음 블록체인의 기본적인 개념을 살펴보았고, 디지털 데이터의 관리를 위하여 어떤 블록체인 기술을 선택할 것인지, 어떤 구조로 설계할 것인지 검토하였다.

블록체인 방식을 이용하여 로그를 관리한다면 압수한 디지털 데이터의 폐기 문제나 법정에서 사용될 증거의 보관 연속성 입증 등을 해결할 수 있을 것으로 기대한다. 최근 디지털 데이터의 대량성으로 인하여 정보 획득에 긴 시간이 소요되거나 전문 인력에 의한 기술적 조치가 필요한 경우가 점점 많아지면서, 대량의 데이터 복제본을 생성하여 압수하는 추세이다. 이러한 경우에는 불가피하게 범죄사실과 관련성에 대한 구분 없이 임의의 전자 정보가 복제되는 경우도 있으며 보관에 어려움이 있는 경우도 있다. 대법원 판례와 서울중앙지방법원의 지침에 따르면 사건과 관련성이 없는 전자정보는 불가피하게 압수하였다고 하더라도 삭제·폐기하여야 한다. 이에 검찰에서도 새로운 매뉴얼을 시행하였고, 매뉴얼에 따라 디지털 증거를 등록하기 전에 수사팀에서 압수한 전자정보의 사건 관련성 여부를 판단하고, 압수의 필요성이 없다고 판단되면 D-NET에 등록하지 않도록 하고 있다. 또한 사건 처분 전이나 사건 처분 후에도 사건과 관련 없음이 명백한 자료는 폐기토록 하고 있다. 폐기 후 본 논문에서 제안하는 방식으로 폐기하였음을 확인한다면 효율적인 방법이 될 것이다. 또한 디지털 증거는 데이터 수정에 취약하기 때문에 법원에 증거로 제출될 때까지

보관의 연속성을 지켜 보관해야 한다. 압수한 디지털 데이터에 적법한 권한이 있는 자만 접근하였고, 무분별한 복제나 수정이 없었음을 보장하여야 증거로 사용할 수 있을 것이다. 블록체인을 활용한 디지털 증거 관리 방식은 보관·폐기의 확인 외에도 보관의 연속성을 보장하고, 사생활 보호 등에 대한 우려가 있는 자료가 어떻게 보관되었는지 확인해준다.

블록체인을 활용한 디지털 증거 관리 방식을 적극적으로 사용하기 위해서는 기술적인 연구와 이를 뒷받침하는 관련 법리를 준비하는 것이 중요한 과제가 될 것이다. 본 논문이 디지털 증거 관리에 일조하여 실체적 진실의 발견을 위한 수사·공판에 도움이 될 뿐만 아니라, 피압수자의 기본권 보호에도 도움이 되는 합리적인 방법으로 활용되기를 기대한다.

참 고 문 헌

Ⅰ. 국내자료

1. 이재상, 조균석, 형사소송법, 박영사 (2015)
2. 탁희성, 압수물로서 디지털증거의 보존 및 처리에 관한 법제도 개선, 한국형사정책연구원 (2011)
3. 대검찰청, 과학수사 실무 매뉴얼 (2014)
4. 대검찰청, 각국의 압수물 관리 · 처리 실태 및 효율적인 압수물 관리 · 처리 방안, (2011)
5. 대검찰청, 압수대상으로서의 디지털 증거 관리 매뉴얼 (2016)
6. 금융보안원, 블록체인 개요 및 활용사례, 보안연구부 (2015)
7. 금융보안원, 블록체인 및 비트코인 보안 기술, 보안연구부 (2015)
8. 금융보안원, 국내외 금융분야 블록체인 활용 동향, 보안연구부 (2015)
9. 안드레아스 M. 안토노풀로스, 비트코인, 블록체인과 금융의 혁신, 고려대학교 출판문화원 (2015)
10. 장상귀, 디지털 증거의 증거능력에 관한 연구, 법학실무연구회 (2009)

Ⅱ. 국외자료

1. Eoghan Casey, Digital Evidence and Computer Crime, (2011)
2. KORBIT, Block Chain Primer (2016)
3. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2009)

Ⅲ. 판례자료

1. 헌법재판소 2012. 12. 27. 선고 2011헌마351 결정
2. 대법원 2011. 5. 26. 2009모1190 결정
3. 대법원 2015. 7. 16. 선고 2011모1839 전원합의체 결정

Ⅳ. 기타

1. <https://ko.wikipedia.org/wiki/디지털> 2016.11.14. 최종검색
2. <https://ko.wikipedia.org/wiki/공개_키_암호_방식> 2016.11.14. 최종검색
3. <https://ko.wikipedia.org/wiki/비트코인> 2011.11.14. 최종검색
4. <http://www.seunghwanhan.com/2016/10/public-blockchain-and-private-blockchain.html> 2011.11.14. 최종검색
5. <https://brunch.co.kr/@jeffpaik/5> 2011.11.14. 최종검색
6. <https://letstalkpayments.com/an-overview-of-blockchain-technology/> 2011.11.14. 최종검색

Abstract

Suggestion of safe management of confiscated digital data

Seong Hoon, Lim
Department of Mathematical Information Science
The Graduate School of Convergence Science & Technology
Seoul National University

As the use of digital devices becomes more popular, there are more and more cases in which human actions are recorded in digital form while we are not aware of them. As much information is being recorded as digital data, digital forensics plays an important role in criminal investigation.

Recent Supreme Court cases have provided some important guidelines for digital evidence. The first is that, in principle, seizure of the storage medium itself is prohibited. The second is that even if copying, searching or outputting a storage medium or a copy to an investigation agency's office, etc., the right of participation of the person to be attacked must be ensured. Third, the investigative body should dispose of electronic information irrelevant to the incident. In response to the ruling of the Supreme Court, the Seoul Central

District Court enforced the “New Practice Guideline on the Warrant for the Seizure of Electronic Information.“ According to the above guidelines, electronic information is subject to confiscation in principle. In addition, the confiscated electronic information shall be made up of a detailed list and issued to the person to be confiscated, and the information irrelevant to the alleged crime shall be deleted and destroyed. If the Supreme Court precedents and the above guidelines are combined, it will be confiscated with only relevant information related to the crime, and the intention is to delete or discard irrelevant information even if it is inevitably confiscated.

As the Supreme Court ruled that electronic information is subject to seizure search, a management method considering the characteristics of digital evidence is needed. Digital evidence can only be used as evidence if it meets the requirements of authenticity and integrity. To ensure the integrity and authenticity of digital evidence, we maintain continuity of archiving by generating and verifying the hash value when acquiring digital data and integrating it into the server until digital evidence is submitted to court.

In addition, due to the massive amount of digital evidence, it can take a long time to acquire information or it may face various problems such as requiring technical measures by skilled workers. In this case, it is difficult to achieve the purpose of confiscation by outputting and duplicating only data related to crime facts in the field. In the end, inevitably, when a large amount of electronic information is confiscated, the problem of discarding irrelevant

information remains.

Therefore, the prosecution conducted a “Digital Evidence Management Manual as an Object of Confiscation“ to register and dispose of the confiscated electronic information in Digital Dignity Network (D-NET), and prepared a plan to manage the electronic information which is irregular. In this paper, we propose a method for objectively and scientifically verifying digital evidence when it is discarded or archived. In the case of discarding, the hash value of the discarded log and the hash value stored in the block chain are compared with each other to manage the digital evidence management If there is no abnormality, it will be more efficient.

In addition to confirming storage and disposal, the digital evidence management method using the block chain guarantees the continuity of archiving, and it confirms how the data of concern about the privacy protection are stored. In order to actively use the digital evidence management method using the block chain in practice, it will be important to prepare technical research and related legal principles to support it. We hope that this paper can be used as a reasonable way to help protect the basic rights of the intruders as well as help in the investigation and trial for the discovery of substantive truth in cooperation with digital evidence management.

keywords : Digital Evidence Management, Confidential Spill Prevention, Block Chain
Student Number : 2015-26065